RTO-TR-049
AC/323(IST-008)TP/15

RTO-TR-049

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

BP 25, 7 RUE ANCELLE, F-92201 NEUILLY-SUR-SEINE CEDEX, FRANCE

RTO TECHNICAL REPORT 49

Intrusion Detection: Generics and State-of-the-Art

(la Détection de l’intrusion: Modèles génériques et état de l’art)

This Technical Report has been prepared by Task Group on Information Assurance, which is RTG-003 under the RTO Information Systems Technology Panel.

Published January 2002

Distribution and Availability on Back Cover

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burder for this collection of information is estibated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burder to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) 01-01-2002	2. REPORT TYPE	3. DATES COVERED (FROM - TO) xx-xx-2002 to xx-xx-2002

4. TITLE AND SUBTITLE Intrusion Detection: Generics and State-of-the-Art Unclassified	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME AND ADDRESS Research and Technology Organisation North Atlantic Treaty Organisation BP 25, 7 rue Ancelle, F92201 Neuilly-sur-Seine Cedex, Francexx	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS ,	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This report presents the generics and describes state-of-the-art of Intrusion Detection Systems (IDSs). The report also aims at highlighting some of the issues for use of co-operative IDSs in a coalition environment. To facilitate the discussions and analysis, generic models are introduced. This includes the IDS generic model, where an IDS consists of sensor, management and alarm-processing components and optionally may have reaction, deception, and visualisation components. To show how IDSs can be deployed and operate at different locations in a Communication and Information System (CIS), a generic model based on the CIS architecture is introduced as well. Finally, these generic models are extended as a way to look at intrusion detection in a coalition environment. The report describes and discusses IDS analyser techniques, examples of commercial products, standardisation efforts, and several issues regarding interoperability, management, performance, availability, and privacy. Furthermore IDSs are discussed in relation to early warning of an intrusion in a CIS, and the need for evidence collection after an intrusion has occurred. The discussions and analysis show that IDSs are useful in detection of intrusions in a CIS, even though several black spots are identified. It is also shown that IDS deployment and co-operation in coalition environments still need a great deal of research, development, standardisation, together with policy and management considerations.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Public Release	18. NUMBER OF PAGES 50	19. NAME OF RESPONSIBLE PERSON Fenster, Lynn lfenster@dtic.mil
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

This page has been deliberately left blank

Page intentionnellement blanche

RTO-TR-049
AC/323(IST-008)TP/15

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

BP 25, 7 RUE ANCELLE, F-92201 NEUILLY-SUR-SEINE CEDEX, FRANCE

RTO TECHNICAL REPORT 49

Intrusion Detection: Generics and State-of-the-Art

(la Détection de l’intrusion: Modèles génériques et état de l’art)

by:

R. Coolen
H.A.M. Luiijf

TNO Physics and Electronics Laboratory
The Netherlands

with contributions from:

A. Møller, DDRE, DE, S.K. Dahel, DREO, CA
V.K. Taylor, DREO, CA, G. Eizenberg, ONERA, FR
H.K. Nichols, DERA, UK, G. Hallingstad, NDRE, NO
M.H. Kang, NRL, US, W. Stein, FGAN, GE
P.J.M. Veugen, TNO, NE, W.M.L. Verspaandonk, TNO, NE

This Technical Report has been prepared by Task Group on Information Assurance, which is RTG-003 under the RTO Information Systems Technology Panel.

The Research and Technology Organisation (RTO) of NATO

RTO is the single focus in NATO for Defence Research and Technology activities. Its mission is to conduct and promote cooperative research and information exchange. The objective is to support the development and effective use of national defence research and technology and to meet the military needs of the Alliance, to maintain a technological lead, and to provide advice to NATO and national decision makers. The RTO performs its mission with the support of an extensive network of national experts. It also ensures effective coordination with other NATO bodies involved in R&T activities.

RTO reports both to the Military Committee of NATO and to the Conference of National Armament Directors. It comprises a Research and Technology Board (RTB) as the highest level of national representation and the Research and Technology Agency (RTA), a dedicated staff with its headquarters in Neuilly, near Paris, France. In order to facilitate contacts with the military users and other NATO activities, a small part of the RTA staff is located in NATO Headquarters in Brussels. The Brussels staff also coordinates RTO's cooperation with nations in Middle and Eastern Europe, to which RTO attaches particular importance especially as working together in the field of research is one of the more promising areas of initial cooperation.

The total spectrum of R&T activities is covered by the following 7 bodies:

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS Studies, Analysis and Simulation Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These bodies are made up of national representatives as well as generally recognised 'world class' scientists. They also provide a communication link to military users and other NATO bodies. RTO's scientific and technological work is carried out by Technical Teams, created for specific activities and with a specific duration. Such Technical Teams can organise workshops, symposia, field trials, lecture series and training courses. An important function of these Technical Teams is to ensure the continuity of the expert networks.

RTO builds upon earlier cooperation in defence research and technology as set-up under the Advisory Group for Aerospace Research and Development (AGARD) and the Defence Research Group (DRG). AGARD and the DRG share common roots in that they were both established at the initiative of Dr Theodore von Kármán, a leading aerospace scientist, who early on recognised the importance of scientific support for the Allied Armed Forces. RTO is capitalising on these common roots in order to provide the Alliance and the NATO nations with a strong scientific and technological basis that will guarantee a solid base for the future.

The content of this publication has been reproduced
directly from material supplied by RTO or the authors.

Published January 2002

ISBN 92-837-1079-7

Printed by St. Joseph Ottawa/Hull
(A St. Joseph Corporation Company)
45 Sacré-Cœur Blvd., Hull (Québec), Canada J8X 1C6

Intrusion Detection: Generics and State-of-the-Art

(RTO TR-049 / IST-008)

Executive Summary

Internal and external threats to NATO Communication and Information Systems (CISs), amplified by interconnection with the CISs of other nations and organisations, increase the risk of intrusions or other irregularities. A prerequisite for effective counter-measures is early, and often real-time warnings about intrusions in NATO and interconnected coalition CISs. Intrusion Detection Systems (IDSs) are technical means that focus on the detection of intrusions in CISs.

In principle, the deployment of IDSs in NATO CISs and coalition CISs provides a good basis for early warning and intrusion detection. Consequently, a timely and adequate reaction to an intrusion or attack can be prepared, maintaining the operational status of a CIS while gathering evidence. However, the discussion and analysis in this report show that available commercial IDSs are not yet capable of providing a complete intrusion detection solution.

The discussions and analysis in this report are based on IDS generics. The report introduces an IDS generic model, where IDSs consist of sensor, management and alarm-processing components and optionally may have reaction, deception, and visualisation components. To show how IDSs can be deployed and operated at different locations in a CIS, a generic model based on the CIS architecture is introduced. Finally, the generic models are extended as a way of looking at intrusion detection in a coalition environment.

In summary, the following observations and black spots are indicated regarding commercial IDSs. These observations provide challenges for both the (NATO) IDS-research & development community and the operational community:

- If NATO uses special applications or services in a CIS, tailor-made or -configured IDS-sensors may be required to analyse the full scope of potentially hostile activity.
- Different IDSs use different protocols for alarm messages and management. NATO should stimulate and support standardisation efforts in this field.
- In theory, only the so-called anomaly-based IDSs are able to detect new and unknown intrusions. However at present, anomaly-based IDSs lack practical applicability, because of high false alarm rates.
- Misuse-based IDSs, which have a database with intrusion information (~ signatures), that are updated regularly can detect a wide range of known intrusions and variants. However, regular updates of signatures are required, i.e. NATO should choose either to institutionalise continuous development of signatures or to stimulate IDS manufacturers in continuous updating of signatures.
- The evaluation of the effectiveness and manageability of different IDSs is an important step in obtaining a good intrusion detection solution. Currently evaluation efforts are limited.
- From the perspective of early warning, IDSs should have sophisticated correlation techniques and should be able to co-operate. These capabilities are still limited.
- IDSs can be used to supply information about intruders. In particular, an IDS could supply and store evidence that could be used in criminal and civil legal proceedings. It is noted that in military environments prevention or evasion of attack often has a higher priority than post-event legal remedy or assistance of law enforcement.
- IDSs should be designed to be resistant against attacks, in particular against denial-of-service attacks, floods of false alarms, and anti-IDS techniques.

- If NATO plans to use IDS to detect intrusions in NATO and coalition CISs, as proposed in the generics in this report, NATO should consider the development of policies in which intrusion information will be shared with coalition partners. Commercial IDSs however at present lack the means to implement such policies.
- The visualisation of intrusions in combination with the capacity and performance of networks and links between networks can be a useful feature of IDSs, because of the rapidly growing complexity and size of networks.
- An IDS should be organisationally embedded with enforcement of the applicable privacy laws and regulations.

Although already useful in detection of intrusions, there is room for large improvement of commercial IDSs. In particular improvements concerning deployment, communication and co-operation in and between NATO CISs and coalition CISs are needed.

la Détection de l’intrusion: Modèles génériques et état de l’art

(RTO TR-049 / IST-008)

Synthèse

Les menaces internes et externes auxquelles les systèmes d’information et de communication de l’OTAN (CIS) sont exposés, en plus des interconnexions qui existent avec d’autres CIS d’autres pays et d’autres organisations, font accroître le risque d’intrusions et d’autres irrégularités. La transmission d’alertes avancées, ou en temps réel en cas d’intrusions dans les CIS de l’OTAN ou dans les CIS interconnectés des pays d’une coalition est l’une des conditions indispensables à l’obtention de contremesures efficaces. Les systèmes de détection d’intrusions (IDS) sont des moyens techniques conçus spécifiquement pour la détection d’intrusions dans un CIS.

En principe, le déploiement d’IDS dans les CIS de l’OTAN et de ceux d’une coalition offre de bonnes garanties de transmission d’alertes avancées et de détection d’intrusions. Ainsi, une réaction adéquate et en temps voulu en cas d’attaque ou d’intrusion peut être préparée, pour assurer la disponibilité opérationnelle d’un CIS, tout en recueillant des informations. Cependant, la discussion et l’analyse présentées dans ce rapport démontrent que les IDS disponibles sur étagère ne représentent pas encore la solution du problème de la détection d’intrusions.

Les discussions et analyses contenues dans ce rapport sont basées sur des éléments génériques. Le rapport présente un modèle d’IDS générique, composé d’éléments de détection, de gestion et de traitement d’alerte, avec en option des possibilités de réaction, de déception et de visualisation. Un modèle générique, basé sur les architectures CIS est décrit pour illustrer les possibilités de déploiement et de fonctionnement d’IDS à différents niveaux dans un CIS. Enfin, le concept de modèles génériques est étendu à la détection d’intrusions dans un environnement de coalition.

En résumé, les observations et les obstacles suivants ont été signalés en ce qui concerne les IDS disponibles sur étagère. Ces observations posent des défis tant pour les chercheurs au sein de la communauté de recherche et développement IDS de l’OTAN que pour les exploitants.

- Dans le cas où l’OTAN disposerait d’applications ou de services spéciaux dans un CIS, il pourrait s’avérer nécessaire de prévoir des capteurs faits sur mesure ou configurés IDS pour analyser l’étendue réelle d’activités potentiellement hostiles.
- Différents IDS utilisent des protocoles différents selon qu’il s’agisse de messages d’alerte ou de gestion. L’OTAN doit encourager et soutenir les efforts consacrés à la normalisation dans ce domaine.
- En principe, seuls les IDS dits “fondés sur les anomalies” sont en mesure de détecter des intrusions nouvelles et inconnues. Cependant, à présent, les IDS fondés sur les anomalies posent des problèmes d’applicabilité en raison de leurs taux de fausse alarme élevés.
- Les IDS fondés sur l’emploi abusif, qui ont une base de données contenant des informations sur les intrusions (- signatures), qui sont mises à jour régulièrement, peuvent détecter un grand éventail d’intrusions et de variantes. Cependant, des mises à jour régulières des signatures s’imposent, c’est-à-dire que l’OTAN doit décider soit de prendre en charge le développement continu de signatures, soit d’encourager les fabricants des IDS à mettre à jour les signatures en permanence.
- L’évaluation de l’efficacité et de la capacité de gestion des IDS représente une étape importante de la recherche d’une solution valable du problème de la détection d’intrusions. Les efforts actuellement consentis dans le domaine de l’évaluation sont limités.
- Du point de vue des alertes avancées, les IDS doivent intégrer des techniques de coopération et de corrélation sophistiquées. Pour le moment, ces capacités restent limitées.
- Les IDS peuvent fournir des informations sur les intrus. En particulier, un IDS pourrait archiver et fournir des témoignages susceptibles d’être utilisés dans le cadre de poursuites judiciaires et criminelles.

Il est à noter que dans le contexte militaire la prévention ou l’évitement d’attaques a souvent la priorité sur les actions en justice après l’événement ou l’aide à l’application de la loi.

- Les IDS doivent être conçus pour résister à l’attaque et en particulier aux attaques de refus de service, à la transmission massive de fausses alarmes et aux techniques anti-IDS.
- Si l’OTAN prévoit la mise en œuvre de systèmes IDS pour la détection d’intrusions dans les CIS de l’OTAN ainsi que dans ceux d’une coalition comme il est proposé dans ce rapport, elle devrait réfléchir au développement de politiques permettant de partager des données sur les intrusions avec les éventuels partenaires d’une coalition. Cependant, les IDS actuellement disponibles sur étagère ne sont pas adaptés à la mise en œuvre de telles politiques.
- La visualisation d’intrusions, associée aux capacités et performances des réseaux et des liaisons entre réseaux est une fonctionnalité intéressante des IDS, vu l’évolution rapide de la complexité et de la taille des réseaux.
- Du point de vue organisationnel, les IDS doivent être associés à la mise en application des lois et règlements relatifs au respect de la vie privée.

Les IDS du commerce, bien que déjà très utiles pour la détection d’intrusions, peuvent être considérablement améliorés, en particulier en ce qui concerne le déploiement, la communication et la coopération entre les CIS de l’OTAN, ainsi qu’avec les CIS d’une coalition.

Click inside the blue boxes to view the corresponding section

Contents

APPENDICES

Foreword

In 1999, the Information Systems Technology (IST) panel of the NATO Research and Technology Organisation (RTO) established the Task Group on Information Assurance (TGIA). The TGIA research area is Information Assurance[1], i.e. those measures taken to protect information in CISs against accidental or malicious attacks regarding availability, integrity, and confidentiality. The background is the extensive and increasing use of electronically based information systems, which has simultaneously created new capabilities and new vulnerabilities. It is critical to the future of NATO, that systems remain robust and retain the confidence of the users. The proliferation and diversity of attacks on CISs has already been reported in the civilian sector, and is expected to increase. NATO's increased use of COTS information technology and dependency on CIS for weapons, intelligence, communication, and logistics will increase vulnerability to attacks. The work of TGIA is intended to help provide advice to NATO on tools and methods for countering these threats.

The main objectives of TGIA are to identify and explore Information Assurance technologies that may impact operation of NATO and coalition CISs. To fulfil these objectives, TGIA has a plan of work with 3 themes. The first theme is a Boundary Control study, which includes investigation of architectures of boundary controllers to facilitate secure and effective communication between NATO and coalition CISs. The second theme is an Intrusion Detection study with methods and tools to prevent, detect, and even react on attacks to NATO and coalition CISs. The third theme is a workshop on the application of Information Forensics (~ Inforensics) technology for analysis of attacks on a CIS.

TGIA currently works on these 3 themes, and this report on "Intrusion Detection: Generics and State-of-the-Art" reflects the result of the initial work on the Intrusion Detection theme. The main purpose is to give an overview of state-of-the-art of IDSs and identify some of the challenges and benefits of deployment in NATO and coalition CISs. To facilitate the discussion and analysis of IDSs, generic models of IDSs are introduced. These generic models include the components of an IDS, the architecture for deployment in a single CIS environment, and an extended model related to deployment in coalition CISs.

As the discussions and analysis of this report show, IDS deployment in a coalition environment still need a lot of research, development, standardisation, policy, and management consideration, etc. This report with intrusion detection generics and state-of-the-art should yield a good basis for further improvements of these deficiencies, in particular for the research and development community. The follow-on work of TGIA regarding the Intrusion Detection theme is expected to further address some of the coalition issues. Besides, it is the hope that the CIS operational community is able to benefit from this report by getting a better understanding of the (potential) capability of IDSs deployed in a coalition CIS environment.

As Intrusion Detection technology constantly improves, this kind of State-of-the-Art report reflects the state at time of writing, i.e. last half of year 2000. Any subsequent developments are not taken into account.

Finally, it should be mentioned that NE was the lead for this report, and carried out major part of the work. The other members of TGIA co-operated with contributions, suggestions, and ideas, either at discussions at TGIA meetings or by direct interaction.

Alfred Møller
Chairman of the TGIA

[1] Within this report the term "Information Assurance" is used, even though NATO uses the term "Assurance of Information"

Membership of Task Group on Information Assurance (IST/RTG-003)

Vincent Taylor
Informations Operations Section
Defence Research Establishment Ottawa (DREO)
3701 Carling Ave
Ottawa, ON, K1A 0Z4
Canada
E-mail: Vincent.Taylor@dreo.dnd.ca

Sahnoune (Karim) Dahel
Informations Operations Section
Defence Research Establishment Ottawa (DREO)
3701 Carling Ave
Ottawa, ON, K1A 0Z4
Canada
E-mail: sahnoune.dahel@dreo.dnd.ca

Alfred Moeller
Danish Defence Research Establishment (DDRE)
Ryvangs Alle 1 - PO Box 2715
DK-2100 Copenhagen 0
Denmark
E-mail: avm@ddre.dk

Gerard Eizenberg
ONERA/DTIM
2 Avenue E Belin
BP4025
31055 Toulouse Cedex 4
France
E-mail: Gerard.Eizenberg@cert.fr

Willi Stein
C/o FGAN/FKIE
Neuenahrer Str. 20
D-53 343 Wachtberg-Werthhoven
Germany
E-mail: stein@fgan.de

Eric Luiijf
TNO Physics and Electronics Laboratory
Telecommunication and Security Division
PO Box 96864
2509 JG The Hague
The Netherlands
E-mail: luiijf@fel.tno.nl

Rutger Coolen
TNO Physics and Electronics Laboratory
Telecommunication and Security Division
PO Box 96864
2509 JG The Hague
The Netherlands
E-mail: coolen@fel.tno.nl

Geir Hallingstad
Norwegian Defense Research
Establishment (FFI)
PO Box 25
N-2027 Kjeller
Norway
E-mail: geir.hallingstad@ffi.no

United Kingdom currently not represented.

Julie Ann B. Tarr
Code 5544
Naval Research Laboratory (NRL)
4555 Overlook Avenue, SW
Washington, DC 20375-5337
United States
E-mail: tarr@itd.nrl.navy.mil

1 Introduction

Increasingly, NATO Forces operate in multinational coalitions and connect the NATO (nation) networks to non-NATO nations (NNNs), non-NATO international organisations (NNIOs), and non-governmental organisations (NGOs). Increasingly, operational requirements demand the sharing of information and integrating communication and information systems (CISs) of NATO nations and/or other coalition Forces. The use of interconnected modern information and communication technologies enhance the situational awareness and the strive for information dominance.

Internal and external threats to CIS, amplified by interconnecting with CIS of other nations and organisations, require early and often real-time warnings about intrusions and other irregularities in the NATO CIS as well as effective counter-measures. This to reduce the risks associated with potential unauthorised access to, compromise of, and control over NATO information and that of its members.

Intrusion Detection Systems (IDSs) are technical means that focus on the detection type of measures against intrusions in and to a CIS.

This report describes generic models of intrusion detection in order to classify commercial and state-of-the-art IDS as well as (re)active and other components that can be part of an IDS. A further purpose of these generic models is to have a common starting point for the interworking of IDSs both in a single CIS environment and in a coalition environment. Another aim of this report is to identify black spots in IDSs and to state issues and problems that require further research and development.

The primary target audience of this report is researchers of IDSs. This report should help as a starting point for more detailed research in order to improve IDS designs and interoperability.

The secondary target audience is people involved in Information Operations, security staff, CIS planning/implementation authorities, procurement authorities and NATO security accreditation authorities. This report should help to understand how IDSs operate, what the benefits and problem areas of IDSs are, and how IDSs may help them to reduce certain risks and to increase intelligence on possible intentions of intruders/attackers.

In chapter 2, terms are explained and definitions are presented. The next chapter discusses the place of intrusion detection in the set of security measures that form the security incident-cycle. In chapter 4, a generic model of an IDS is described. Chapter 5 contains an introduction of an architecture model for the interworking of IDSs in a CIS. Chapter 6 discusses intrusion detection protecting a coalition set of CISs, comprising a joint IDS-network, and including an extended generic model. In chapter 7, the internal analysing techniques of IDSs are described.

Chapter 8 describes and discusses examples of current IDS products. The various standardisation efforts around for example the interoperability of IDSs are described in chapter 9. To explain why IDSs are required in order for a timely response, chapter 10 discusses the need for early warning in a CIS. Then chapters 12 and 13 discuss performance, availability, management, and other issues concerning IDSs. Chapter 14 discusses recent and future research and developments. Finally, chapter 15 summarises the conclusions.

2 Terms and definitions

In literature, different terms and definitions are used for intrusion and intrusion detection. In this report definitions are chosen in accordance with [1] and [2], but with a focus on the military operational CIS environment.

Attack: A deliberate intrusion in a CIS.

Attacker: The person, group, organisation or state that performs an attack.

Defender: The person, group or organisation (i.e. NATO agency or NATO nation) that is responsible for the target CIS.

Intruder: The person, group, organisation or state responsible for an intrusion.

Intrusion: A deliberate or accidental unauthorised access to, activity against, and/or activity in, a CIS.

Intrusion Detection: The process of identifying that an intrusion has been attempted, will occur, is occurring, or has occurred.

Target: The CIS that an intrusion is aimed at.

Note that the definition of an intrusion includes intrusions that have an intentional or unintentional intend, harmful or harmless consequences, and concern both intrusions by insiders and outsiders by definition respectively affiliated to the defender organisation or not.

Both unintentional intrusions and attacks can result in damage. This damage can concern the availability, integrity and/or confidentiality of the CIS. To do damage to the integrity or confidentiality of information requires gaining access to the system containing the information. This is usually one of the first stages of the intrusion. The attacker intrudes the defenders' CIS with the goal to read, modify, and delete information and/or control the CIS.

An intrusion that is directed to the availability of the system does often *not* require gaining access to a system as a prerequisite.

3 Security measures

In this chapter, intrusion detection is positioned as one of the security measures against an intrusion. The purpose of this chapter is to see where IDSs fit in to the overall range of security measures. The measures are presented using the security incident cycle, which is visualised in figure 1.

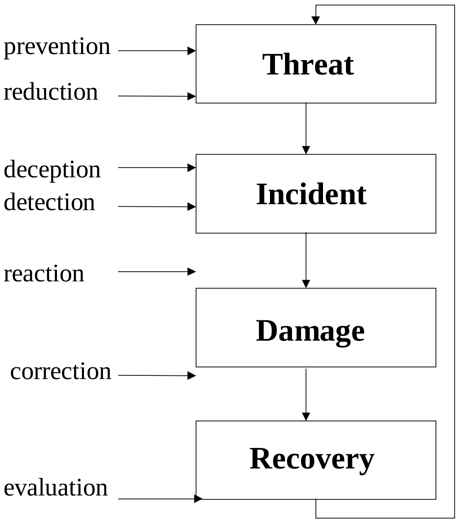

Figure 1: *Security incident cycle*

The intrusion part of the cycle consists of four elements: the threat, the incident (e.g. an intrusion), the occurrence of damage, and the recovery. The following different types of security measures are related to these elements: prevention, reduction, deception, detection, reaction, correction, and evaluation.

The security incident cycle has to deal with threats to the confidentiality, integrity and availability of the CIS. A defender first of all takes *prevention measures*. These measures prevent a threat from becoming a reality. An example of a prevention measure to protect an internal network is a Boundary Protection Device (BPD). Another example of a prevention measure is scanning for known vulnerabilities in a CIS and thereafter correcting these vulnerabilities by implementing patches or changing configuration parameters.

Reduction measures are measures that are performed in advance to reduce possible damage of an intrusion. Examples of reduction measures are redundant systems, limitation of bandwidth, and regular back-ups.

Deception measures are a special type of security measures. They have the purpose to give false information to intruders, to reduce the possibility of an intrusion, to allow easier detection of an intrusion, to slow intruders down, or to obtain operational benefits over the intruding party.

Prevention, reduction and deception measures reduce the probability and the impact of an intrusion. However, this does not exclude possible occurrence of an intrusion. Therefore, the defender takes *detection measures*.

All intrusions have to be detected as early as possible, as will be explained at length in chapter 10. In this way, the defender does not loose valuable time over the intruder. This time can be used to identify the intruder and to take more extensive prevention, reduction, and deception measures to minimise damage and to maximise reaction. Intrusion detection is the main focus of IDSs. However, there is a tendency that other security measures such as reaction and deception are also incorporated in IDSs. In the generic model of an IDS presented in the next chapter, this will be taken into account by incorporating reaction and deception properties. However the main focus in this report is the detection nature of an IDS.

After an intrusion is detected, the defender takes *reaction measures*. These reaction measures can be repressive in order to block the repetition of the intrusion. The reaction measures can also include tracing an intruder. Furthermore, if the operational authority for the CIS decides to start a process to press charges against an intruder/attacker, Inforensics[2] evidence often needs to be collected between the moment of the first intrusion related events, a successful intrusion in, and the recovery of the CIS. A workshop on Inforensics is organised by TGIA[3].

When an intrusion results in damage to the integrity or availability of information, the next step in the security incident cycle is to take *correction measures* to undo at best the damage that was done. The operational status of vital parts of the CIS has to be reconstituted as soon as possible. This is where *reduction measures* such as back-ups prove their usefulness.

The final step in the security-incident cycle consists of an effectiveness *evaluation* of the security measures taken. Questions might be: what went well and what went wrong? And what lessons can be learned and how to prevent a reoccurrence of the intrusion in the future?

Note that prevention, reduction, and detection measures should be designed according to the defence-in-depth principle [4]. That is the attacker or intruder should have to overcome multiple lines of defence before he/she is able to breach the confidentiality, availability, or integrity of the NATO, NATO member's or coalition partner CIS(s).

4 Generic model of an IDS

In this chapter a generic model of an IDS is introduced. The purpose of this model is to function as a common viewpoint for the study and discussion of functionalities and components of IDSs. Different components are distinguished and described in a logical order. Furthermore some additional definitions are provided. The generic model of the IDS is visualised in figure 2.

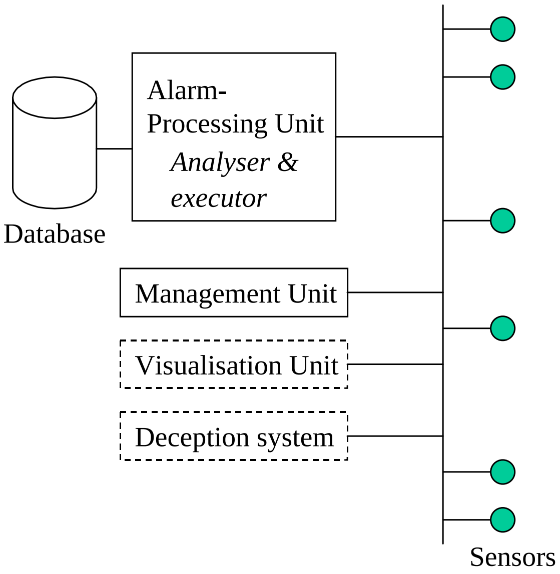

Figure 2: IDS Generic model

4.1 Sensors

Sensors are the generic components of an IDS that collect *activity*. This activity can include network traffic, user misbehaviour, application misbehaviour and so forth. In the intrusion detection community it is common to distinguish between two types of activity: network activity and host activity.

[2] Information forensics, reconstruction and recovery: the application of forensic techniques to investigate crimes involving, either directly or indirectly, information and communication technology (ICT).
[3] A workshop on Inforensics is organised by TGIA (~ NATO/RTO/IST/RTG-003) in November 2001.

Network activity: the activity present at the network is the network traffic, which can be categorised in:

- Low level protocols (ISO layers 2, 3 and 4 e.g. TCP, UDP);
- Application and service level protocols (e.g. SMTP, HTTP, FTP);
- Content (of e.g. e-mail or web pages).

Host activity: at the hosts (including clients, servers and routers) several forms of activity are present, caused by:

- Users: the person operating on a host, e.g. identified by a login account;
- Systems: hardware, operating system;
- Network services (e.g. PKI, DNS);
- Applications: e-mail, web browsers, and so forth.

Examples of sensors are network interfaces in promiscuous mode and tools that read log-files. An IDS can have multiple sensors. Based on the type of activity the sensors collect, the following classification of IDSs is made:

1. *Host-based IDS (HIDS)*: look at activity on a host.
2. *Network-based IDS (NIDS)*: look at the network traffic either in (near) real-time or via e.g. log-files.
3. *Hybrid* IDS: has sensors collecting host and network activity. *Kernel-based* monitoring as for instance by the Linux Intrusion Detection System (LIDS) [46] is considered to be a special hybrid case as both network and host system intrusion activity is monitored within one host system.

4.2 Alarm-processing unit

The alarm-processing unit is the generic component of an IDS that pre-processes and analyses the activity collected by the sensors. Furthermore the alarm-processing unit controls the reaction to be taken by the IDS in reaction of a detected intrusion. The alarm-processing unit is subdivided in three elements.

4.2.1 Analyser

There exist two main classes of alarm-processing units based on the technique they use for analysing activity to detect intrusions [1]:

1. *Anomaly-based:* the ‘normal behaviour’ of the system is known and an intrusion is detected, when the activity differs in some sense from the normal behaviour.
2. *Misuse-based*: the (type of) intrusion is known and stored beforehand (as a so-called signature). An intrusion is detected when the activity matches the known intrusion signature.

The different analyser techniques that are used by an alarm processor are discussed in more detail in chapter 7.

Human interaction with the analyser can be an important aspect of analysing activity. Therefore the alarm-processing unit should be able to cope with human intervention in the decision process of whether activity indicates an intrusion.

Before the collected activity is analysed it is usually pre-processed to get a uniform input in the actual analyser.

A characteristic of an IDS is the frequency of the analysis. Three categories are distinguished:

1. *Continuously*: events are collected and thereafter analysed, as they occur, - often in real-time.
2. *Periodically*: events are collected and analysed periodically from the subject. An example is system log files that are analysed every hour.
3. *Initiated under special circumstances*: e.g. when the system administrator suspects an intrusion.

4.2.2 Knowledge and storage database

The information about known intrusions and/or the normal behaviour of the activity is stored in a *knowledge database*. The alarm-processing unit can also store (information about) collected activity in a *storage database* that can be of interest in the future.

4.2.3 The executor

When the IDS decides that certain activity indicates an intrusion, an alarm is generated by the executor component. This alarm can either be *passive* or *active:*

Passive: an IDS generates an alarm, which can be a log file message, a pop-up screen, a pager message and so on, or a combination thereof.

Active: the generic model includes IDSs that have (optional) active components that can generate automatic reactive control signals. These control signals could for example tighten a BPD, increase the IDS’ sensitivity, shutdown a connection, divert network traffic to a decoy system or shut down hosts that are under attack.

An IDS can operate in close co-operation with network management systems. Alarms can be incorporated in network management systems. Active IDS-alarm components might send network management control messages to different components of the network.

Besides sending control signals, the executor part of the alarm processing unit is able to send alarm messages to other IDSs. These messages have the purpose to share intrusion related information within and also outside the CIS for example with NATO coalition partners' networks. The alarm messages should be send whenever the IDS detects activity that could indicate an intrusion, in particular a distributed intrusion. Typically, an alarm message contains:

- Time, date, and location of the possibly intrusion related activity;
- Classification of the activity;
- Specific information about the activity; and
- Information about the intruder.

4.3 Management unit

The management unit of the IDS is the generic component that allows the system managers responsible for the IDS to change and manage the:

- IDS' detection behaviour (sensitivity, verification frequency, parameter settings);
- Updating such as the addition of new intrusion signatures;
- Response (active, passive); and
- Availability by rebooting of crashed IDSs and so forth.

In an environment with multiple IDSs, the management units will be able to co-operate, by sharing messages for management control, to facilitate for example central management. This feature will be introduced in the next chapter. The management of IDSs is discussed in more detail in chapter 12.

4.4 Deception systems

As an optional generic component an IDS can contain a deception system. Two different types of deception systems are distinguished: *decoy deception systems* and *information deception systems*.

4.4.1 Decoy deception systems

Attraction of the attacker can be done either actively or passively. In the first case, the defender actively gives away information to the attacker about the decoy deception system. In the second case, the attacker has to find the information him/herself, e.g. in the process of scanning the target network.

Preferably the decoy deception system is a dedicated component. This has the advantage, that all network traffic directed to the system is suspicious and indicates an intrusion. This way not only intrusions can be detected in an early stage by the IDS, but also the entire intrusion can be recorded and hence novel intrusion techniques can be learned.

Detection of an intrusion in an early stage is clearly desirable. When the attacker spends time intruding the deception system, valuable time is gained over the attacker. This time can be used to protect the real CIS and/or to trace the intruder.

The following types of decoy deception systems can be distinguished:

1. *Logging system*: Logs the information about the attacker. An example would be to log all traffic to the telnet port. A possible way to attract attackers would be to send plain text username-password combinations over the network that can be intercepted by the attacker.
2. *Fake system*: Carefully designed to fake a real vulnerable system. An example is a fake pop-server that has part of the protocol implemented. It would take the attacker some time to figure out the system is not a real system. The attacker could be attracted to the system, after a port scan at the POP3-port.
3. *Real system*: A real vulnerable system. For example a host, with a known vulnerable operating system or application. The attacker can e.g. do a port scan to this machine and hack it. The classic example a monitored and controlled attack on a real system can be found in [5].

Decoy deception systems have the following disadvantages. Firstly, when compromised they can be used as a stepping stone to further compromise the CIS. Building the system in a virtual machine (jail) can make this a lot harder for the attacker. Secondly, decoy deception systems add complexity to the CIS. This may lead to increased vulnerabilities. Finally, decoy deception systems have to be managed, which costs resources.

4.4.2 Information deception systems

These systems are lures to give false information to intruders. This type of systems is regarded to be outside the scope of this report, and is mentioned here for completeness only.

4.5 Intrusion visualisation unit

Another optional generic component of an IDS is the intrusion visualisation unit. Because this unit is more relevant when looking at intrusion detection in a CIS environment, it will be discussed in chapter 5.

4.6 IDS overview

This chapter ends with a summary of IDS characteristics, - shown in figure 3. Characteristics of optional components such as the deception system are excluded.

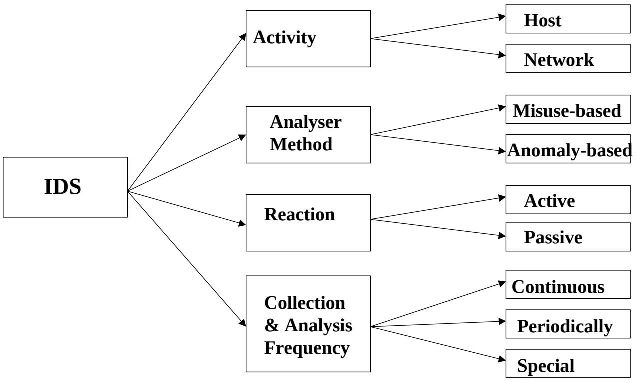

Figure 3: IDS characteristics

5 An architecture for intrusion detection in a CIS

IDSs can be deployed at different architectural locations throughout a CIS. In this chapter, an architecture for the interoperability and management of IDSs in a CIS, is presented. This architecture is based on the IDS generic model from the previous chapter, and proposes a way ahead for research, development, and deployment of intrusion detection in CISs. The problem of where to place IDSs in a specific CIS is however not discussed. Mainly since this is a highly situation dependent problem

Firstly, in section 5.1, a CIS network model with a CIS connected to an external network is presented.

Next, in section 5.2, IDSs are positioned at locations in the CIS and in the external network. These IDSs are connected via a *communication channel* and will function as sensors for what we call the CIS IDS (CIDS).

Finally, section 5.3 discusses issues concerning the different possible positions in the CIS for the sensor IDSs, and section 5.4 is about deception IDSs.

5.1 A CIS network model

The network model, which is the basis for the CIDS architecture, consists of an external network connected to an internal CIS by Boundary Protection Services (BPS). Examples of BPS are the BPD and virus-scanners. The network model is in accordance with the NATO network model for interconnection [3]. An example is a NATO or NATO member nation's CIS connected by a firewall to the Internet.

More general network models could be constructed. For example a network could include a so-called demilitarised zone (DMZ). The DMZ is a network that has a different, in practice 'lower', security posture than the internal CIS.

However a more general network model, does not influence the fundamentals presented in this report, since the generic models are relevant to any security posture in any network.

Both the external network and the CIS contain hosts (clients and servers) and active networks components like switches and routers.

In the CIS, two types of intrusions can be distinguished:

1. *External intrusions*: all intrusions that originate at the external network side of the BPS and that pass through the BPS.
2. *Internal intrusions*: all intrusions that originate within the internal CIS or BPS.

These definitions include intrusions that enter the CIS via other means, such as a back-end modem connection or off-line media (e.g. a floppy). If these intrusions do not pass (authorised) BPS, they are regarded as internal since they require insider faults or misuse.

5.2 CIS IDS (CIDS)

IDSs operate at a *location* in the CIS environment with the internal, external or DMZ networks. Examples of locations are switches, routers, PCs connected to transmission media, database servers, and/or parts of the BPS.

By positioning several IDSs at locations in the CIS, a system for intrusion detection in a CIS is realised. We call this the CIS IDS (CIDS).

The IDSs that collect activity at a location in the CIS environment are called *sensor IDSs*. The alarm processing unit of a sensor IDS can send alarm messages. Alarm messages are send via a communication channel and form the input of the alarm-processing unit of the CIDS. Hence the sensor IDSs function as sensors for the CIDS, and the CIDS will have similar generic components as the sensor IDSs, including optional components. This results in a hierarchical model of IDSs, in which the higher level CIDS has the lower level sensor IDSs as components. This is what we will call the CIDS generic model, which is a single layer hierarchical model.

The CIDS architecture focuses on the generics of IDSs, which include communicating and co-operating sensor IDSs in a CIS. The distinct advantages this provides are:

- Correlation of data is feasible; without correlation of hybrid data, sophisticated and low frequency attacks can not be detected. This is addressed in chapter 10.
- Centralised alarm processing and alarm analysis.
- Intrusion visualisation at different levels in the hierarchical model.
- (Central) management of the lower level sensor IDSs.

Figure 4 visualises the architecture of the CIDS generic model.

The management unit of the CIDS is able to communicate with the management units of the sensor IDSs. This allows for central management of all IDSs in the CIS.

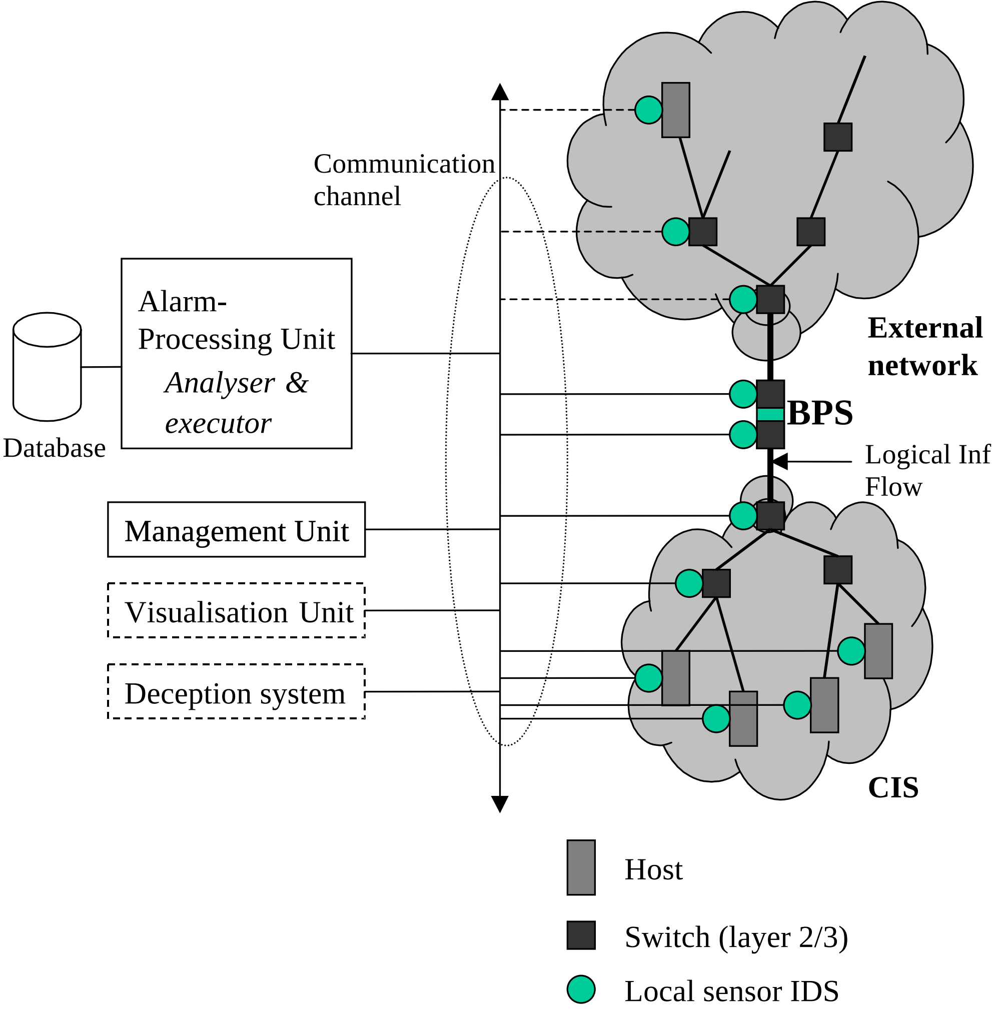

Figure 4: CIDS architecture

In the next subsections the communication channel and intrusion visualisation unit are described.

5.2.1 Communication channel

Sensor IDSs can communicate with the CIDS and with other components of the CIS. Alarm messages can be send to the CIDS, reaction control signals can be send to components of the CIS (e.g. a BPS component), and messages for management control can be shared between management units of IDSs and the CIDS. The communication channel that is used to communicate these messages and signals, can either be in-band or out-of-band:

- *In-band*: the network that might be under attack is used for the IDS communication. The disadvantage is that a denial-of-service attack might suppress the internal IDS communication and alarm signals and thus central visibility of an intrusion that takes place at the same time.
- *Out-of-band*: a separate network or communication community (e.g. virtual LAN) is used for the internal IDS communication and alarm communication. The disadvantage is that a separate (logical) network is required.

5.2.2 Intrusion visualisation

In order to obtain informational situation awareness, intrusion visualisation in the CIS network is important. In the generic models for Intrusion Detection, the optional intrusion visualisation unit takes care of this. It can combine information of intrusions with other information such as the network (link) performance (e.g. availability and usage).

The visualisation component can be tightly linked to an IDS alarm processor, but preferably be an open component, which can fuse information from various lower level sensor IDSs, and other type of sources such as network performance monitors.

5.3 Locations of sensor IDSs

The sensor IDSs can be located at different architectural positions in the CIS, BPS and (if possible) even in the external network. The choice of locations for the sensor IDS is an important one, since different intrusions result in different activity at different locations. In this report the problem of choosing IDS locations within a CIS is not solved, however certain issues regarding the different possible positions are discussed in this paragraph.

Consider an external intrusion. The path of intrusion-related network traffic starts at an external user at an external host and is transmitted to the BPS. If it passes that line of defence, the network traffic continues its path to an internal host, resulting in intrusion activity that is visible in the CIS network.

Consider an internal intrusion. The intrusion can originate at the same host as the target itself (*local intrusion*), in which case there might be no intrusion related network activity. Furthermore, internal intrusions can originate at a client host in the CIS and traverse the internal network to the target host.

At all the locations corresponding to a specific (local) internal or external intrusion, activity related to the intrusion can be collected and analysed. The following sections summarise these different locations at which a sensor IDS can operate. Issues related to the specific location are discussed.

5.3.1 External host

At the external host, activity can be collected from the user and/or applications responsible for the intrusion and network packets containing the intrusion. Observe that:

- It can be hard to place and/or manage sensor IDS at the external host, if the location is outside controlled area. Examples are hosts outside NATO, NATO member nation’s, or coalition partner’s control.
- An intruder can possibly detect and be able to disable the IDS.
- Some intrusions can easily be recognised at the external host, but it might be harder or even impossible to recognise along the route to the target. An example is a DoS-attack, where the IP-address is spoofed.

5.3.2 External Network

At the external network activity can be collected at active network components like switches and routers, and in boxes or PCs connected to transmission media (e.g. network cards in promiscuous mode). Observe that:

- It can be hard to place and/or manage sensor IDSs in/near the external network components and network transmission media.
- Some intrusions can easily be recognised at the external network, but it might be harder or even impossible to recognise at other locations. A good example is an attack using spoofed IP packets.
- A tremendous amount of network traffic can pass at the described locations, including traffic that is not intended for the CIS (including a possible DMZ). The IDSs might not be able to keep up with this amount of traffic.
- Denial-of-service attacks can be detected at active network components. Furthermore these active components could be involved in prevention and reaction of such attacks.

5.3.3 Boundary Protection Services (BPS)

At the BPS, all the traffic between the external network and the CIS passes and can hence be collected. Observe that:

- The amount of traffic that passes the BPS can be high, hence IDSs might not be able to keep up with the traffic.
- Encrypted traffic can't be decrypted and hence not analysed at the BPS. In theory, the keys and algorithms to encrypt are available at the CIS (otherwise the encryption would be of no use), however it is often undesired and/or unfeasible to implement the decrypting in the BPS.
- An IDS can be located at the front or the rear of the BPS. In the first case intrusions can be detected even if they are stopped by the BPS. In the second case, traffic speed is often lower, since the BPS typically filters network traffic.

5.3.4 CIS network

At the CIS activities can be collected at the active network components like switches and routers, and boxes or PCs connected to transmission media in the route of the network traffic (e.g. network cards in promiscuous mode). Observe that:

- Deployment of sensor IDS should be easy, as the defender is in control of the CIS.
- To collect all traffic requires at least a sensor IDS in each segment of the network. In a network where each host is switched, this requires as many sensor IDSs as hosts. A solution would be to plug an IDS into a switch and let it collect traffic from all network segments.
- Encrypted traffic is hard to deal with, as is the case with IDSs at the BPS.
- Special IDS in boxes or PCs connected to transmission media in the route of the network traffic are often easier to protect from attacks than the sensor IDSs that are situated in the intruder's host or targeted hosts. This is because these sensor IDSs can be built as dedicated systems and be stealthily present in the network.

5.3.5 CIS hosts

At the CIS hosts activity of user, network traffic, services, systems, and application activity can be collected. User activity can be analysed for suspicious behaviour and misuse. Network services activity can be analysed for abnormal traffic (volume per second, time-of-day), weird connectivity and probing. Systems can be checked for (side) effects of an intrusion, for example by regularly checking a checksum of executables. Furthermore traffic can be analysed for intrusion symptoms. Observe that:

- This is the only location where network, services, hardware, operating system, application and user activity can be collected.
- Encrypted traffic can more easily be dealt with if an end-user station is concerned. An example is virus/Trojan Horse verification after decrypting an e-mail attachment.
- The bandwidth of the traffic is relatively low.
- Because the intruder can have either an authorised or an unauthorised access to the target host, it is important that an IDS at the target host is attack proof.
- The host is the only location where local intrusions can be detected.

5.4 Locations of decoy deception systems

The intrusion-detection deception systems can be at best situated at the locations, where normally the main (external) targeting efforts of attack probing take place. In case of a CIDS, the deception systems can for example be located near a webserver.

6 Intrusion detection in a coalition environment

In the previous chapter we saw that sensor IDSs can send alarm messages to the CIDS and that the CIDS management unit can communicate with the different management units of the sensor IDSs. The CIDS has an architecture similar to the individual sensor IDSs, which makes the generic models a single layer hierarchical model.

In a similar way different alarm messages from CIDS corresponding to different CISs can be send to a higher level IDS by adding an extra layer to the model. For instance, this could be a NATO wide IDS where different NATO members can send alarm messages to and that allows management of intrusion detection at NATO level. Another example is a Military Operation IDS, where CISs of different NATO members, NNNs, NGIOs and NGOs involved in an operation are shared in order to have operational awareness of enemy information warfare activities.

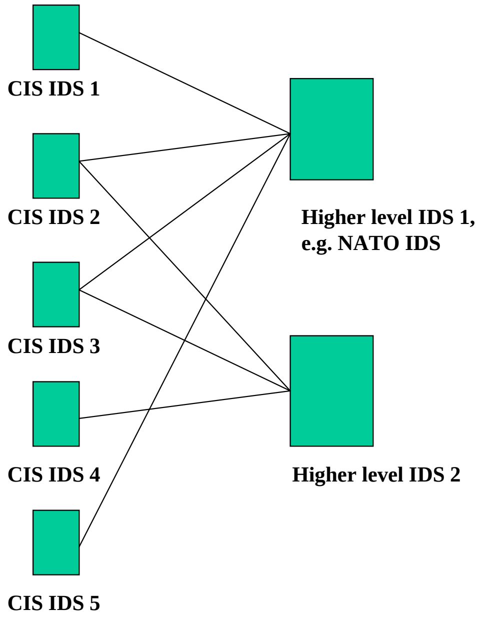

Figure 5: Example with level 2 CIDSs

The generic models can be extended even more by adding more levels and by allowing for merged IDS generic models. This means that organisations can choose to share information to multiple higher level CIDSs. The organisation responsible for the CIS has to decide on what information it is willing to share to different co-ordinating organisations (NATO, UN, and so forth). This policy should then be implemented in the CIDS architecture. Figure 5 visualises the extended CIDS generic model (with 2 levels).

An important aspect of the sharing of alarm and reaction messages is the management of the communication channel used. In particular the security of the alarm and reaction communication is a very important aspect. Otherwise the remedy may be worse than the disease, e.g. blocking by the intruder of the alarm processor or the reaction channel by overloading the information channel.

The added layer to the hierarchical model proposes a way of looking at intrusion detection in a coalition environment. We have chosen a top-down hierarchical structure for two reasons. Firstly this is an efficient structure from management and control perspective. And secondly this structure is chosen because it corresponds with the structure of most government and commercial organisations. In particular it corresponds to the NATO command structure.

Another possible way of organising the IDSs would be a decentralised structure, where the IDSs form a loosely coupled network in which every intrusion detection system can ‘choose’ the intrusion system it wants to share information with.

The deployment and development of IDSs according to the hierarchical model presents a challenge for research, development and operation of IDSs within NATO.

7 Analyser techniques

The 2 main classes of IDS analyser techniques (misuse and anomaly detection) are elaborated in the following sections. Besides a strict version of the anomaly-detection technique is presented, but first the difficulty of analysing activity with respect to false alarms is discussed.

7.1 False alarms

No alarm-processing unit is infallible in analysing potential intrusion related activity. The alarm processing unit in an analyser may fail to detect intrusions, or sound the alarm, when no intrusion has occurred. Four cases in the operation of an analyser are distinguished (Table 1).

Table 1: Four cases in the operation of an event analysis.

	Intrusion	**No Intrusion**
IDS Alarm	An intrusion has occurred, and the IDS generated an alarm *(correct alarm)*	No intrusion has occurred, but the IDS has (erroneously) detected an intrusion *(false alarm)*
IDS Rejection	An intrusion has occurred, but the IDS has not generated an alarm *(false rejection)*	No intrusion has occurred and the IDS has not detected an intrusion *(correct rejection)*

Related to these four cases two parameters of an IDS are defined:

- The *accuracy* of an IDS: the number of *correct alarms* divided by the number of *correct alarms plus false alarms*; is a parameter for the relative number of correct alarms. The more accurate an IDS is, the fewer false alarms it generates and the higher this parameter is.
- The *completeness* of an IDS: the number of *correct alarms* divided by the number of *correct alarms plus false rejections*; is a parameter for the relative number of correct alarms. The more complete an IDS is, the fewer intrusions remain undetected and the higher this parameter is.

In the ideal case, an IDS would be 100% complete (it detects all intrusions) and 100% accurate (it produces no false alarms). However detecting an intrusion is a very difficult task, this comes partly forth from the base-rate fallacy problem [6]. The base-rate fallacy problem shows the need for very accurate IDSs. If an IDS generates too many false alerts, the operating and managing personnel will have no confidence in the system!

7.2 Misuse detection

Analysers that use the *misuse detection* method operate by searching for very explicit activity and/or patterns of activity. Misuse detection is also called detection-by-appearance.

A number of known *intrusion patterns* (also known as intrusion *signatures* or *rules*), that specify the features, conditions, arrangements and interrelationships among activity that leads to break-in or other misuse are stored beforehand in the IDSs knowledge database. The IDS collects activity and looks whether one of the stored intrusion patterns occurs. If an intrusion pattern is detected, the IDS will generate an alarm.

A detection-by-appearance IDS can only detect *known* intrusions, but once it detects an intrusion, it can usually specify exactly how the intrusion has occurred.

There exist a number of techniques used by misuse detection IDS, some of these are described in appendix D.2.

> Example*:*
>
> *A remote user is transferring files using ftp from a UNIX machine with IDS. The IDS detects the commands being given by the user for a number of possible pre-defined intrusions. One of these pre-defined intrusions is the command "get /etc/passwd". If this command is ever executed, an intrusion is flagged, as the remote user is trying to obtain the password file from the machine.*

In a sense the misuse detection concept is paradoxical, because the intrusions have to be known beforehand. One could argue that a CIS should not be vulnerable to known intrusions. However, in practice it is impossible to remove all vulnerabilities from a system. Mainly since this is time, knowledge, and resource consuming. Because it is not feasible to make the CIS proof to all known vulnerabilities, the misuse detection IDS can certainly provide an important role to detect known intrusions, intrusion attempts and other intrusion related activity.

An advantage of a misuse-detection IDS is that it is not only useful to detect intrusions, but that it will also detect intrusion attempts; a partial signature may indicate an intrusion attempt. Furthermore, the misuse-detection IDS could detect port-scans and other events that possibly precede an intrusion.

A disadvantage of a misuse-detection IDS is that only known intrusions are detected. No protection is offered against novel attacks, or new variants of existing intrusions. More crucially, a small variation in the form/structure of an attack can invalidate a signature. This is discussed in more detail in chapter 13, section 3.

Examples of misuse-detection IDSs are:

- *Application-level firewalls:* which check communication at the application level. An example is the string get /etc/passwd in the ftp protocol, which means that a user is trying to obtain a password file from the target machine, which usually indicates an intrusion.
- *Virus checkers*: which check files and memory for the occurrence of specific strings typical for a given virus strain.

Misuse detection is the most used technique in current NIDSs. There are two different types of NIDS, smart and raw, depending on whether they look at patterns in low-level protocol activity or application-level protocol activity [7].

Smart: IDSs that have logic implemented that understands the target protocol. They will parse the request and perform (optimised) signature matching based on known rules pertaining to the protocol. They will attempt to behave like a real web server would behave, at the expense of additional code and slowness. RealSecure is an example of a smart IDS (see chapter 8).

Raw: Also referred to as 'packet grep' style IDSs, they typically just scan the unprocessed raw data for key strings. The benefit of this is speed only. The term raw is not used in a derogatory manner, but rather to identify that these IDSs usually deal with the raw data directly, rather than interpreting the protocols. Example IDSs of this type are Dragon and Snort (see chapter 8).

7.3 Anomaly detection

Event analysers that use the *anomaly detection* method operate by examining the behaviour of the activity. Anomaly detection is also known as detection-by-behaviour.

The ‘normal’ behaviour of activity is stored beforehand in the IDS. The activity is then continuously collected and analysed to see whether its behaviour significantly deviates from the stored behaviour. The IDS sees significant deviation between these behaviours, as a (possible) intrusion.

> Example*:*
>
> *User* jdoe *normally logs in 4-6 times per week, commencing around 8:30 in the morning, and logging off between 16:00 and 22:00. In these sessions, he runs MS-Word about 70% of the time and Netscape Navigator about 20% of the time. If* jdoe *one day logs in at 02:00, or if he suddenly starts using network management applications, the IDS may signal this as an intrusion alarm.*

An anomaly detection IDS is confronted by two related problems:

1. *Description problem*: How to describe the behaviour of activity in an effective and efficient manner?
2. *Comparison problem*: Given a stored behaviour pattern of activity and a current behaviour, when do these two deviate enough to constitute a possible intrusion?

An IDS based on anomaly detection is classified according to how it deals with these two problems, see [8]. The main problem with anomaly-detection IDSs is that it is hard to describe the ‘normal’ behaviour of activity, because of e.g. the unpredictable behaviour of the end-users. This results, especially in the light of the base-rate fallacy problem, in IDSs generating a lot of false alerts This is the main reason that anomaly detection IDSs are hardly used in practice and are mostly at a research stage. Appendix D.1 elaborates on different techniques used in anomaly-based intrusion detection.

The main advantage of a good working (few false alarms) anomaly detection IDS would be that in a sense ‘unknown’ intrusions can be detected. The systems however detect only the fact *that* an intrusion has occurred rather than *how* it has occurred. This creates a situation where the IDS does not need a priori knowledge of specific security flaws in a CIS.

7.4 Strict anomaly detection

In [6] a strict anomaly detection model is described, which has the distinct feature that it generates no false alarms by definition. In this paragraph, the strict anomaly detection model is described.

Firstly, it is noted that an IDS should not see an attack as a binary *did* / *did not* see an intrusion decision problem. Different forms of attack technique are not equally complex and therefore not equally complex to detect. Hence the IDSs decision problem should be n-valued.

The proposed strict anomaly detection model is as follows. An IDS should use precise definitions of ‘use’ for activity in a CIS, in accordance with security policy. Any deviation of these definitions is a security policy violation.

In case of the normal anomaly detection the ‘use’ behaviour is not strictly defined but merely a description of normal behaviour of activity

The key-advantage of the strict anomaly detection model is that new attacks can be detected, while no false alarms are generated!

Examples of a strict anomaly detection model include:

- In IP-networks, the TCP/IP state-transition diagram could be modelled as a set of ‘use’-rules. The different implementation flavours of TCP/IP stacks could be taken into account. Any deviation of the state-transition diagram would indicate an attack.
- Alternatively, a stateless approach could be taken by defining the allowable variation in each field of the TCP header.
- A more broad and important example is in the scenario when the IDS is deployed on the inside of a BPS. The ‘use’ set could consist of the reverse of the BPS policy. This is perfect example of a defence-in-depth strategy, where the IDS is an extra line of defence behind the BPS.

An example of a product that uses a strict anomaly detection concept is Finjan’s SurfinGate (see chapter 8).

8 Current IDS products

In this chapter current IDS products are described, with the purpose to illustrate some of the main techniques and concepts used. This is done in order to be able to identify some black spots in IDS products in relation to the generic models. Based on available products, the description is divided into IDSs (section 8.1) and products that can be used to add deception functionality to intrusion detection in a CIS (section 8.2), followed by a discussion of the black spots (section 8.3).

> Disclaimer: The content of this chapter is *explicitly not* a recommendation, nor a critical and complete comparison of IDSs. All information that is stated about the *example* IDSs is from documentation from the Internet, mostly specified by the IDS vendors.

8.1 Examples of sensor IDSs

In this section some commercial and freeware IDSs are described. These are: Dragon, ICEcap, Cisco Secure IDS, Snort, and RealSecure. A few other IDSs are briefly mentioned as well.

- **Dragon**

Dragon (Enterasys) is a hybrid IDS consisting of the Dragon Sensor, the Dragon Squire, and the Dragon server. The Dragon Sensor is a NIDS sensor. When it detects an intrusion, the Dragon Sensor can send pages, email messages, take action to stop the event and record it for future forensic analysis. Dragon Squire is a HIDS sensor. It looks at system logs for evidence of malicious or suspicious application activity in real time. It also analyses key system files for evidence of tampering. Dragon Squire can also analyse firewall logs, router events and other network components that can speak SNMP or Syslog. The Dragon Server facilitates secure management of all Dragon Sensors and Dragon Squires. It also aggregates all alerts into one central database so that disparate attack information can be correlated. Firewall, NIDS, and HIDS events are all correlated at the Dragon Server. The Dragon Server includes a variety of reporting and analysis tools as well as the ability to customise alerts via email, SNMP or Syslog messages. All signature libraries for Dragon Sensor and Dragon Squire can be automatically updated once per day.

- **ICEcap Security Suite**

The ICEcap Security Suite (Network ICE) is a hybrid IDS that consists of the following components that all work together. The ICEcap Manager deploys, manages, and updates the BlackICE Agents, Sentries and Guards from a single manager throughout the network. ICEcap Manager consolidates alerts, logs hostile activity, and forwards information to other applications, including enterprise management consoles. Collective Awareness allows one Agent, Sentry or Guard to alert all others to potentially dangerous activity anywhere in the network. BlackICE Agents deployed on every server, notebook and remote user system protect the entire corporate network. BlackICE Agents centrally report to the ICEcap Manager, and enforce user, group, or enterprise-wide security policies set by ICEcap Manager. BlackICE Agents run on Solaris, Linux and Windows platforms. BlackICE Agents are compatible with VPN clients. BlackICE Guard identifies and removes attacks from a segment before the attack can succeed. BlackICE Sentry provides network-based intrusion detection on Gigabit and Fast Ethernet segments without the need for expensive hardware-based solutions. BlackICE sentries report suspicious or hostile traffic directed against any device, from printers to notebooks to mainframes, back to the ICEcap Manager. InstallPac is a remote installation tool that can push BlackICE Agents and Sentries, as well as updates, out across the network.

- **Cisco Secure IDS**

The Cisco Secure IDS (Cisco) is a NIDS, consisting of Sensors and a Director. The Sensor is a network appliance that uses a rules-based engine to analyse large volumes of IP network traffic and Syslog information from Cisco routers. Intrusions are translated into meaningful security events, which it forwards to a Director. The Sensor can also log security data, cut TCP sessions, and dynamically manage a router's access control lists to shun intruders. The Director provides a centralised graphical interface for the management of security across a distributed network. It can also perform other important functions: data management through third-party tools, access to the Network Security Database (NSDB), remote management of Sensors, and send pages or e-mail to security personnel when security events occur. The Cisco Secure IDS Director scalability and performance can centrally monitor the activity of dozens of Cisco Secure IDS Sensors located on different types of network connections. For extremely large, distributed networks with complex alarming and communication requirements, the Cisco Secure IDS Director can be implemented in a multi-tiered hierarchy, enabling a virtually unlimited number of Sensors to be managed. Because the Director also remotely controls the configuration of the Cisco Secure IDS Sensors via an intuitive Java-based GUI integrated into a network management system, an organisation can manage the security of its connections from one centralised location. The Cisco Secure IDS Director can also feed alarm information into an adjacent database archive. Information such as the origin, type, destination, and time of attacks is all logged for trend analysis and may easily be used to generate custom graphs and reports.

- **Snort**

Snort (freeware) is a misuse-based lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort uses a flexible rules language to describe traffic that it should collect or pass. Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or WinPopup messages to Windows clients. Snort has no central management and alarm processing features. However efforts have already been taken to implement this feature in Snort. A package called Snortnet is able to manage and process information from different Snort NIDSs. Special about Snort is the fact that it is a freeware tool. Since it is signature based it requires that signatures are available in the public domain. There is a large attack signature database called Whitehats (www.whitehats.com) on the Internet that has Snort signatures. Because of the open nature of this database, where the Internet community shares their knowledge on intrusions, this database is large and update.

- **RealSecure**

Realsecure (ISS) is a hybrid IDS. It consists of Network sensors, OS sensors, and a manager. The Network sensor collects raw, unfiltered network traffic, looking for patterns, protocol violations, and repeated access attempts that indicate malicious intent. The OS sensors perform real-time intrusion analysing, detection, and prevention of malicious activity by analysing kernel-level events and host logs. When RealSecure detects unauthorised activity, it can respond in a number of ways, automatically recording the date, time, source, and target of the event, recording the content of the attack, notifying intrusion detection personnel, reconfigure a firewall or router, suspending a user account, or terminate the attack. The RealSecure manager provides the capability to manage both types of sensors from the same user interface. Both types of sensors use the same alarm formats, report to the same database, and use many of the same reports.

- **Other sensor IDS products**

Other examples of NIDSs include:

- Cybertrace (Ryan Networks).
- Netprowler (Axent).
- Centrax (Cybersafe).
- Network Flight Recorder (NFR).
- eTrust (Computer Associates).

Other examples of HIDSs include:

- Tripwire (Tripwire).
- Intruder Alert (Axent).
- Virus-scanners. Examples are McAfee and Norton.
- Finjan Surfinguard (Finjan) is based on strict anomaly detection. It operates as a HTTP proxy and checks Java applets and scripts according to a strictly defined security policy. For example scripts that access the network or the local disk can be regarded as an intrusion.

Some of these products co-operate in hybrid IDS solutions. Tripwire is available as an integrated component of Centrax and Intruder Alert can co-operate with Netprowler. Finally eTrust has an integrated anti-virus engine.

8.2 Examples of deception IDS

In this section some commercial deception IDSs are described.

- **Fred Cohen’s Deception Toolkit (DTK)**

In the case of DTK, the deception toolkit is intended to make it appear to attackers as if the system running DTK has a large number of widely known vulnerabilities. DTK's deception is programmable, but it is typically limited to producing output in response to attacker input in such a way as to simulate the behaviour of a system, which is vulnerable to the attackers’ method.

- **Specter**

A Specter system consists of a dedicated host with the Specter software. The host can be connected to the network where potentially intruders can be expected. This usually is as close to the external network as possible and could be outside the BPS or in a DMZ. Then the Specter software comes into action. It simulates a complete system. It offers common TCP/IP based services that appear perfectly normal to the intruders, but in fact are traps for them to tap into, mess around and leave traces. All this without even knowing that they are connected to a Specter system which does none of the things it pretends to do but instead logs everything and notifies the appropriate system or security managers. The SPECTER system can even investigate automatically the originators while they are still playing around without having a clue what's really going on.

- **CyberCop Sting**

CyberCop Sting provides a unique extension to traditional intrusion detection methods by creating a virtual network of decoy routers and servers on a host. The Sting server is used to discover would-be hackers, and logs attack efforts to help determine their origin, whether they originate from outside, or even inside the network environment. CyberCop Sting provides vital evidence collection to catch unauthorised users putting production systems and data at risk.

8.3 Discussion

Ideally the location and the choice of sensor IDSs is such that at least theoretically all internal and external intrusions can be detected. For network activity this requires that the chosen IDSs should be able to analyse low level protocols, application level protocols, and content. For host activity it requires that user activity, hardware activity, operating system activity, services activity and performance, and application activity are looked at. Furthermore it requires that the location of the IDSs is such that all activity related to internal and external intrusions can be analysed.

Although some commercial IDSs combine HIDS and NIDS sensors and even virus scanners, there will often be no commercial solution that looks at all activity relevant for an organisation. In particular in military CIS environments where GOTS products and tailor-made applications are often used. These require tailor-made or –configured sensor IDSs. However a major problem with commercial systems is that the different systems use different and sometimes proprietary protocols for alarm messages and management. This implies that different products, in particular tailor-made products, can not be combined in one IDS solution, which provides central management and central intrusion visualisation. So it is not possible to have an IDS solution in a CIS, that combines the ‘best’ sensors for different types of activity and that still fits in the CIDS generic model. A widely supported standard in intrusion detection could resolve this problem. Next chapter discusses the issue of standards.

Another problem is that it is difficult to evaluate IDS. Independent evaluations of the products are necessary to be able to choose the most effective products available. Especially the accuracy and completeness of the IDS analyser are important. Are all intrusions detected? And is the false alarm rate not too high? In 1998 and 1999, the Lincoln Laboratory of MIT conducted a comparative evaluation of IDSs developed under DARPA funding. The 1998 effort was a good start and gave some nice comparative results [9], but it also got some critique on the design of the evaluation [10]. The 1999 effort has shown some improvements [10,11]. However objective standardised evaluation techniques and procedures are still far from realised in the intrusion detection community.

Most commercial IDSs are misuse based and therefore require signatures of attacks. It is important that IDS knowledge database is quickly updated for signatures of new attacks. Although most of the commercial IDS products have some automated method for updating the signatures, the organisation deploying the IDS is still dependant on the speed with which the IDS vendor updates the underlying knowledge database. The same problem is seen with anti-virus software.

Intrusion visualisation is important, because of the rapidly growing complexity and the size of networks. Although commercial systems use intrusion visualisation techniques, there is room for improvement.

A final problem addressed here is that commercial products do not correspond to the (extendend) CIDS generic models. As far as known, they do not propagate alarm messages, control signals, and management signals through different layers of the hierarchical model. Cisco Secure IDS does have the possibility to build a hierarchical IDS structure, however it is not possible to implement policies on what information to share with higher level IDSs and what control and management signals to allow in a CIS.

In chapters 12 and 13 other problems such as performance issues, management issues and so forth are addressed.

9 Intrusion Detection standards

There are no accepted international or de facto standards yet in the IDS community. The first work that was done on standardisation, were the proposed CIDF and CIDL standards. At present the IETF is working on a standard for sharing alarm-messages. Furthermore ISO/IEC is working on a framework document. The following sections describe these standardisation efforts in more detail.

9.1 Common Intrusion Detection Framework (CIDF)

The Common Intrusion Detection Framework (CIDF) [12] was an effort started by DARPA. According to the CIDF-standard: an IDS consists of discrete components that communicate via message passing. Several kinds of components are envisaged:

- Event generators (colloquially “E-boxes”)
- Event analysers (“A-boxes”)
- Event databases (“D-boxes”)
- Response units (“R-boxes”)

All four kinds of components exchange data in the form of *Generalised Intrusion Detection Objects (GIDOs)* which are represented via a standard format. A GIDO encodes the fact that some particular occurrence happened at some particular time, or some conclusion about a set of events, or an instruction to carry out an action.

Event generators produce GIDOs but do not consume them. Their task is to sample the particular environment they are specialised for, and turn occurrences in that environment into CIDF GIDOs for use by other components. Analysers take in GIDOs, and analyse them as to their significance (policy violations, anomalies, and intrusions). Their conclusions are turned out as yet other GIDOs. Event databases store activity for later retrieval.

Components are logical entities and may represent anything, which produces or consumes GIDOs. A component might be implemented as a single process on a computer, or might be a collection of many processes on a number of computers.

9.2 Common Intrusion Specification Language (CISL)

Common Intrusion Specification Language (CISL) [12] is being developed by the CIDF community to describe intrusion events. The document describes a language that can be used to disseminate event records, analysis results, and countermeasure directives amongst intrusion detection and response components.

9.3 IETF

Within the Internet Engineering Task Force (IETF, www.ietf.org) an Intrusion Detection Working Group (IDWG) is formed. This working group was formed because the IETF did not find the CIDF specifications suitable for becoming an Internet standard for the exchange of information about intrusions. This was mainly because the CIDF standard was similar to, but not completely in line with the eXtensible Mark-up Language (XML).

The purpose of the Intrusion Detection Working Group is to define data formats and exchange procedures for sharing information of interest to IDSs, and to management systems that may need to interact with them. The Intrusion Detection Working Group co-operates with other IETF Working Groups.

The outputs of the working group is planned to be:

1. A requirements document, which describes the functional requirements for communication between IDSs and requirements for communication between IDSs and management systems, including the rationale for those requirements. Scenarios will be used to illustrate the requirements.
2. A common intrusion language specification that describes data-formats that satisfies the requirements.
3. A framework document identifying existing protocols that are best used for communication between IDSs, and describing how the devised data formats relate to them.
4. The definition of the Intrusion Alert Protocol (IAP) [43], which is an application-level protocol for exchanging intrusion alert data between intrusion detection elements, notably sensor/analysers and managers across IP-networks. The protocol's design is compatible with the goals for the HyperText Transfer Protocol (HTTP).

9.4 ISO/IEC

ISO/IEC JTC 1/SC 27 works on a technical report [1] that defines a framework for detection of intrusions in IT systems. The technical report focuses on:

- Establishing common definitions for terms and concepts associated with IT intrusion detection;
- Describing a generic model of IDSs;
- Providing high-level examples of attempts to exploit systems vulnerabilities;
- Discussing common types of input data and the sources of intrusion detection analysis;
- Discussing different methods or combinations of methods of intrusion detection analysis; and
- Describing activities/actions in response to indications of intrusions.

The framework explains intrusion detection terms and concepts and describes the relationship among them. Furthermore, the framework addresses possible ordering of intrusion detection tasks and related activities.

10 Early warning

It is important that information about possible intrusions is available as soon as possible. This principle is known as *early warning*. In this chapter IDSs are discussed in relation to early warning, a time-axis model is used to describe the time-line of an attack (~ a deliberate intrusion).

10.1 Time axis model

The stages of an attack are discussed according to an attack time-axis scheme from [13]. This attack scheme is presented in Figure 6.

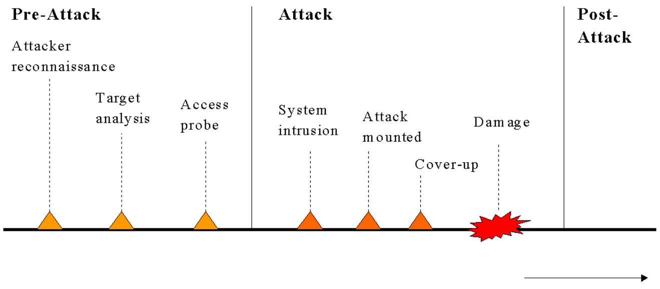

Figure 6: Time axis model of an attack

The actual attack is preceded by a pre-attack stage. The attacker will begin this stage by defining an end-state with regard to the CIS (~ target). This end-state is a clearly defined and obtainable objective. Desired results may be denial-of-service, acquisition of sensitive information, and/or establish and maintain access to the CIS.

After setting the objective the attacker will seek to identify and define problems associated with breaching the target defences, gather information and make assumptions about the CIS, develop possible courses of action (COA), and analyse each COA. In the time-axis model, three steps are distinguished in the pre-attack stage:

1. *attacker reconnaissance,*
2. *target analysis,*
3. *access probing.*

In the first step: *attacker reconnaissance*, the attacker starts acquiring critical information about the CIS. This includes execution of most, if not all, of the following steps: foot printing, scanning, enumeration, vulnerability mapping, and social engineering (i.e. using social skills to obtain info from e.g. employees).

The second step: *target-analysis* consists of analysing the available information, making assumptions and then developing multiple COAs.

In the third step: *access probing*, the attacker tests the COA, and then selects the best COA. The testing is often done, by sending probes to the CIS or by simulating the CIS. For a “complex” attack, the pre-attack stage can last a long time.

In the following stage of the time-axis model, the actual attack start. Hereafter, the attacker will try to cover up the operation and/or leave a backdoor (e.g. a Trojan Horse or a kernel patch) in the system. An attack can be very hard to recognise when the cover up operation is performed well.

After the damage is done, the post-attack stage starts. This is the stage, where the defender will try to take corrective measures and so forth.

10.2 Correlation of data

At most stages of the attack, there is activity in the (target) CIS. The process of interpreting, combining and analysing the information of all available IDS (mainly in the target CIS, but also available information from external networks) is called *intrusion correlation*.

> A series of syslog messages on one system in the CIS suggests strange behaviour. If the messages were only seen on one machine the security manager might decide to ignore the problem. If the problem would be seen on more systems, the security manager would correlate the information and generate an alert.
>
> An attacker first executes a port scan and collects information about services that are operating in the CIS. A period of time later unknown traffic is directed to different servers, coming from the 'port-scan'-network. By correlating the port scan information with the unknown traffic information an alert could be the result.

The time-axis model can be related to the incident cycle from chapter 3. Both models have a point where an intrusion leads to damage. Where the incident-cycle models the defender's actions in the periods of time before and after the damage, the time-axis model shows the attacker's actions for these two periods of time.

The point of detection of the incident from the incident cycle can also be related to the time-axis model. When an attack is detected in the pre-attack stage, this is called *pre-attack detection*. Similarly when an attack is detected in the actual attack stage this is called *attack-detection*. It is also important to recognise that a system was attacked and that possible damage has occurred or that there is a security breach. The detection of an attack in the post-attack stage is defined as *damage detection* or *post-attack detection*. Has crucial information been modified? Is there a backdoor present in the system?

Different sensor IDSs (located in the CIS or even in external network) can collect information from different stages of the attack. To optimally use this information for early warning the CIDS' analyser should be able to correlate the information in real-time. This should especially include information from the pre-attack, since the first signs of an attack are visible in this stage. The information used could be *in-band information* or *all-band information* [14]. In-band information is all information from activity inherent to the target system. All-band information can be any other information that can be used in the correlation, including information from human intelligence sources.

Current IDSs have limited correlation capabilities. Furthermore, as was already noted, the different commercial IDSs are not able to co-operate. With the growing complexity of networks and attacks, there is a need for development of tools that do communicate and share information, e.g. using the CIDF specifications or the coming IETF standards. Also CIDSs should have correlation techniques implemented in their alarm processing units.

11 IDS and evidence

Although the main aim of IDSs is to detect intrusions, a further aim can be to supply information about the intruder. In particular the IDS could supply and store evidence that could be used in criminal end civil legal proceedings [15]. The legal requirements are different for each nation. For example, an important legal requirement is archiving the original raw data, before any processing on this data is done.

In a lot of situations it is important to gather as much information as possible about the intruder, because it is important to know who is intruding the CIS and what techniques and tools are being used. For this purpose an IDS should collect and store data about the intrusion and the intruder. This can include tracing the location of the intruder and obtaining information about the intruders network, tools and so forth.

However in military environments prevention or evasion of attack is often preferable to post-event legal remedy or assisting legal law enforcement. A paradoxical situation arises, since on the whole, the earlier a warning is given and evasive measures are taken, the less likely it is that detailed information on the intruder can be provided.

In [16] observations and conclusions are offered on the redesigning of IDSs as sources of evidence:

- An investigation for the identity of an intruder need not automatically result in the production of evidence that is admissible and believable by a court.
- Evidence acquisition is a separate but related exercise to intrusion detection. It is best carried out against a checklist with the main problems of admissibility, where the main focus of the gatherer is court explanation and presentation.

- Single streams of evidence are unlikely to be adequate to convince a court. Multiple corroborating streams of evidence are required. The feature that links these streams of evidence will usually be day-time clock data; some means of synchronisation is thus necessary.
- If logs are produced from IDS tools, a prosecutor must prepared (and able) to disclose complete details of the tool, and how it was configured and operated. This may have to include details on the topography of the CIS.
- Logging and other intrusion related evidence, will need to be formally produced to court by the people involved in operating and managing the IDS and/or CIS.
- In case of evidence logging on a putative target, arrangements need to be made to prevent compromise of the evidence during attack. A possible arrangement is to record all information on a separate system that can e.g. only download information and hence cannot be compromised, or that digitally signs the information to ensure its integrity.
- Logging evidence should always be 'best', that is, straight from the computer upon which it was created. Even in the case of subsequently processed data and derived data, the raw logs should always be available.
- There should always be a complete chain of custody or continuity of evidence from source to court. This can e.g. be done by statement, entries in registers, and also by using ICT technologies such as write once disks or digital signatures.
- Almost certainly the arrival of IDS tools and procedures that focus on the collection and preservation of evidence will strengthen the IDS market.

Also a research project has recently started,[4] in which an IDS will be developed with the main goal to detect intrusions, but with the second goal to provide evidence that can be used for prosecution of intruders.

12 Management of IDSs

The management of IDSs is crucial for efficient and good deployment of IDSs in military (and also government or corporate) environment. The management of an IDS is divided in four categories [1]:
- Detection management
- Response management.
- Update management.
- Availability management.

Besides the issues of scalability and protection of management operations is described.

12.1 Detection management

Detection management involves communicating with the IDSs via e.g. a graphical user interface that visualises possible intrusions. Furthermore it can involve manual analysis of data by a manager, e.g. to double-check IDSs.

12.2 Response management

The intrusion detection system, when it is signature or rule based, has to be updated very regularly. As we already noted, new attacks arise every moment, hence the updating of signature based IDSs is an ongoing task. The process of updating the system is called update management. Commercial IDSs do not have a continuous 24h updating process of signatures.

12.3 Update management

Once an intrusion is confirmed, Reponses have to be managed. Most of the actions that have to be taken can not be performed automatically by the executor-part of an IDS. The managing of responses that have to be taken as a result of an intrusion include alarm processing, tracing intruders and so forth.

12.4 Availability management

Availability management deals with ensuring that the system is available at all time. Both the hardware and software components can go out of service and then need maintenance. Furthermore IDSs can be under a dos attack.

12.5 Scalability

Central management is an important property for IDSs in a CIS. Especially when scalability of the intrusion detection capabilities are concerned. Maintenance and updating of different systems becomes difficult when network environments are growing and IDSs are not centrally managed.

[4] At Oxford Brookes University

When operating different IDSs in one solution, central management can not be realised. Different IDSs use different protocols for the communication of management information and control messages.

12.6 Management protection

Management operations themselves must be protected from intruders as well. For example if management commands travel over an in-band network, there is a risk that the IDSs themselves get compromised, this includes the vulnerability to DOS attacks. This issue becomes especially important when IDSs are centrally managed via some sort of management system. Authentication and confidentiality can be provided by using encryption, a lot of commercial IDSs already have encrypted communication implemented.

13 Performance, availability and other issues

Commercial IDSs have several performance and availability issues. Besides performance issues arising from high-speed network traffic, we also address performance and availability issues arising from deliberate anti-IDS attacks and techniques.

13.1 Performance

An important design aspect in IDSs is the capability to perform well at the intended locations in the CIS. Especially for IDSs located at high-speed networks, switches and BPS performance becomes an issue. Especially the smart NIDSs need a lot of computational power to perform stateful inspection on the network traffic. Router vendors are at present not able to allocate the necessary computational power to perform these inspections, hence in the foreseeable future there is no hope that IDSs can perform well in high-speed environments [16]. This is a major problem, since when an IDS can not collect all network activity at a location in the CIS, then attacks can pass the IDS without being noticed.

13.2 Availability issues

Another important aspect of an IDS is that it is resistant against DoS-attacks. If an IDS can be attacked and disabled, the system is of no use. For example, IDSs that collect activity from log-files, depend on the logging server working properly. If this server was disabled by a DoS-attack, then the intrusion signals were not logged and hence the attack was not detected.

Furthermore, when parts of a network are under a DoS-attack it is possible that IDS sensors are not capable of sending alarm-messages to the central alarm-processing unit. Using out-of-band communication between sensor and alarm processing unit can solve this problem.

13.3 Anti-IDS techniques

By covering up intrusion patterns with fake traffic IDSs can sometimes be deluded. This problem arises, because an IDS can not see how a particular operating system or service implementation will actually interpret network traffic. This weakness was studied in [17].

Another weakness found in misuse-based IDSs is that there are often techniques to delude the IDSs analyser. This weakness is explained as follows. The same attack can often be performed in several ways, depending on the (often unknown) implementation of the operating system, service, or application that is target of the attack. Therefore an IDS has to have either multiple signatures for an attack, or a good pre-processor that brings different versions of the same attack back to a uniform pattern of activity. Since specifications of the target system of an intrusion are often not known IDSs can often not deal with this problem of multiple attack versions, simply because not all these attack-versions can be foreseen in advance. Whisker is an example of a tool that exploits this problem for attacks on web-servers. As a result of tools like Whisker, pre-processing abilities of IDSs have been improved over the last years [7].

13.4 False-alarms attack

An annoying situation arises when an intruder deliberately set of false alarms. In this situation an actual attack can be flooded in false alarms and resources of an organisation can be misused. Especially in real-time intrusion detection this is major problem, since it will give the intruder a time benefit. Commercial IDSs have as far as known no build in techniques to deal with the problem of false alarms.

13.5 Privacy issues

As intrusion detection requires the monitoring of user (related) activity, there is a privacy issue. As potentially sensitive information is collected and analysed, there may a threat to personal integrity.

The IDS should be designed in line with privacy regulations depending upon the legal system that is in effect. This however can be a problem, since the privacy laws and regulations differ from nation to nation and area-of-operation.

Privacy Enhancing Technologies (PET, [44]) could probably also be used to deal with the issue. This however is a point for further technical and legal research.

13.6 ID Data Sets

There is a need for two types of data concerning intrusion detection:

1. *Data of intrusion patterns* or in other words signatures of attacks and intrusions. IDSs need this data to recognise intrusions. There is an intrusion signature database called Whitehats [18]. This database includes signatures for the public domain NIDS Snort. Because the database is public domain, it is growing rapidly. Perhaps it will be a future public standard.
2. *Data of events* that include simulated intrusions and background noise. Developers of tools and researchers need reliable detailed data of exploits that can be used to make intrusions repeatable and evaluative in laboratory environments. There are limited data sets developed. For example during the Lincoln Labs evaluations simulating data was constructed. However, the development of good real life and widely available data remains a problem.

14 Research

In previous chapters commercial IDS and related issues are described. To complete the state-of-the-art IDS discussion, this chapter briefly describes some of the recent and current intrusion detection research efforts.

In [19] an intrusion detection system is described that uses autonomous-agents technology. The distributed architecture, prototype, and design and implementation experiences are described.

To obtain a denial-of-service resistant IDS architecture, [20] uses mobile-agent technology combined with network topology features.

The Emerald environment is a distributed, scalable tool suite, for network surveillance, attack isolation, and automated response. It uses models from research in distributed high-volume event correlation methodologies [21].

Research in analyser techniques includes [22,23,24]. Techniques such as neural networks, finite automata, and learning programs are used to refine IDSs.

Evaluation research is being performed at MIT Lincoln Labs [9,10,11]. This was discussed in section 8.3.

Intrusion visualisation research includes [25,26]. Techniques such as graph clustering and graph drawing are used to improve the usability and effectiveness of intrusion visualisation.

Other research includes the following topics: logging, attack classification, detection of distributed denial-of-service attacks, tracing of intruders, sensors embedded in applications, and intrusion detection in high-speed networks.

15 Conclusions

Internal and external threats to CISs, amplified by interconnecting with CISs of other nations and organisations, require early and often real-time warnings about intrusions and other irregularities in the NATO CIS as well as effective counter-measures. The incident-cycle describes these different intrusion counter-measures, in particular intrusion detection.

A generic hierarchical model is introduced in this report describing the functionalities related to an IDS, and proposing a starting point for the research, development, and deployment of IDSs in a single CIS and coalition environment.

Overall conclusion is that in principle the deployment of IDSs in single and coalition networks yield a good basis for early warning and intrusion detection, and consequently a more adequate reaction could be prepared, including restoring the operational situation of a system and/or gathering evidence. However the discussion and analysis in this report show that available commercial IDSs are not yet capable of providing a total intrusion detection solution.

Looking at various commercial IDSs, a number of observations are made and black spots have been identified. These observations provide challenges for both the (NATO) IDS research and development community, and the operational community.

IDSs should be able to collect and analyse all relevant low level protocols, application level protocols, content, user activity, hardware activity, operating system activity, services activity, and application activity. This may require tailor-made or -configured IDS sensors for some applications or services.

IDSs are ideally able to detect new and unknown intrusions. In theory, only the anomaly-based IDSs are able to detect new and unknown intrusions. However, at present anomaly-based IDSs lack a practical applicability, because of the high false alarm rates. It remains to be seen whether this problem can be solved with e.g. learning and adapting technologies. One future direction to solve this problem is the usage of IDSs that use the strict-anomaly detection concept. Strict anomaly detection can provide a good extra line of defence in organisations where clear security policies are defined, - although we have not seen any practical results of effectivity and applicability yet.

Although not able to detect new unknown attacks, misuse-based IDSs that are updated regularly with new attack signatures can detect a wide range of intrusions. This includes known attacks, newer variants of attacks, and intrusion attempts. Furthermore the misuse-detection IDS could detect port-scans and other events that possibly precede an intrusion.

Most state-of-the-art IDSs are misuse-based and therefore require signatures of attacks. It is important that signatures from new attacks are updated in the IDS quickly, in order to protect against these attacks. The organisation deploying the IDS is dependent on the speed with which the IDS manufacturer updates the underlying signature database. However most IDSs allow manual creation and updating of rules as well. When deploying misuse-based IDSs, NATO should choose either to institutionalise continuous development of signatures, or to stimulate IDS manufacturers in continuous updating of signatures.

A major problem with current IDS products is that different systems use different protocols for alarm messages and management. This implies that different products, in particular tailor-made products, can not be combined in one IDS solution providing central management and central intrusion visualisation. So it is not possible to have a single IDS solution in a CIS, that combines the ‘best’ sensors for different types of activity and that still fits within the generic model. A widely supported standard in intrusion detection could resolve this problem. NATO should stimulate and support standardisation efforts such as Intrusion Alert Protocol (IAP from IDWG).

Objective standardised evaluation techniques and procedures are still far from realised in the intrusion detection community. Because of the importance of being able to compare the effectiveness and manageability different IDSs, evaluation is an important development and research topic. Preliminary evaluation work has been undertaken by MIT under DARPA funding. NATO should stimulate similar efforts.

Current IDSs have limited correlation capabilities, for example most IDSs do not use sophisticated statistical correlation techniques, when combining information from different sensors in the first place. Furthermore, different state-of-the-art IDSs are often not able to co-operate. With the growing complexity of networks and attacks, and from the perspective of early warning, there is a need for development of tools that do share and correlate information. IDSs should have correlation techniques implemented in their alarm processing units.

Although the main aim of IDSs is to detect intrusions, a further aim can be to supply information about intruders. In particular an IDS could supply and store evidence that could be used in criminal and civil legal proceedings. It is noted that in military environments prevention or evasion of attack often has a higher priority than post-event legal remedy or assistance of law enforcement. This latter issue is part of a TGIA workshop[5].

IDSs should be designed to be resistant against denial-of-service attacks, flood of false alarms, and anti-IDS techniques. If an IDS can be disabled, floods the intrusion detection personnel with false alarms, or can be by-passed by an intruder, then it looses the ability to detect intrusions and hence becomes useless. This is an important issue for further research and development of IDSs.

An IDS should be designed and organisationally embedded with enforcement of the applicable privacy laws and regulations. This could include the usage of privacy enhancing technologies (PET).

Commercial products are not compatible with the CIDS generic model in the sense that they do not propagate alarm messages, control signals, and management signals through different layers of the hierarchical model, with the possibility to implement policies on what information to share. If NATO chooses to go forward with intrusion detection in coalitions, as proposed in the generics in this report, this also is an important issue in development of future IDSs.

Intrusion visualisation can be an important and useful part of IDSs, because of rapidly growing complexity and size of networks. Intrusion visualisation can also help making the management of IDSs easier. Intrusion visualisation needs more emphasis in future IDSs.

[5] A workshop on Inforensics is organised by TGIA in November 2001.

Within Virtual Private Networks and with the growing usage of protocols using encryption, there is a growing need for IDSs that can handle encryption. However this need reduces when cryptography is used only within the context of trusted communication between trusted partners.

Current public research included the topics of intrusion visualisation, evaluation, correlation, and resistance against Denial-of-Service attacks. In this report we have proposed directions for NATO research and stimulation of research and commercial parties. Although already useful in detection of intrusions, there is room for large improvement of commercial IDS especially concerning deployment in and in-between NATO CISs.

This page has been deliberately left blank

Page intentionnellement blanche

Appendix A — References

1. ‘ISO/IEC PDTR 15947, Information technology – Security techniques – IT intrusion detection framework’, ISO/IEC JTC 1/SC 27 N2691.
2. The President’s National Security telecommunications Advisory Committee, Network group Intrusion Detection, ‘Subgroup Report on the NS/EP Implications of Intrusion Detection Research and Development’, December 1997.
3. NATO AC/322 Infosec subcommittee (SC/4), AHWG/4 on the Interconnection of NATO networks documents and working papers, 2001.
4. ‘Technical and Implementation Directive for the Interconnection of Communication and Information Systems (CIS)’, INFOSEC.
5. Bellovin, Cheswick, ‘Firewalls and Internet Security’, Adison-Wesley, 1994.
6. Sasha, Beetle, ‘A strict anomaly detection model for IDS’, Phrack 56, source: www.phrack.com., 6-11-2000.
7. Rain Forest Puppy, ‘A look at Whisker’s anti-IDS techniques’, 1999, source: www.wiretrip.net/rfp/, 6-11-2000.
8. Esmaili, M., R. Safavi-Naini and J. Pieprzyk, ‘Intrusion detection: a survey’. In: S.J. Chung (ed.). Proceedings of the 12th International conference on Computer Communications 21-24 August 1995 in Seoul. Amsterdam, 1995, pp. 409-414.
9. Graf, ‘The 1998 DARPA/AFRL Off-line Intrusion Detection Evaluation’, 1998, source: http://www.raid-symposium.org/raid98/Prog_RAID98/Table_of_content.html, 6-11-2000.
10. McHugh, ‘The 1998 DARPA Off-Line Intrusion Detection Evaluation’, RAID 2000 Proceedings, Lecture Notes in Computer Science, vol. 1907, Springer, 2000.
11. Lippmann et al, ‘Analysis and Results of the 1999 DARPA Off-Line Intrusion Detection Evaluation’, RAID 2000 Proceedings, Lecture Notes in Computer Science, vol. 1907, Springer, 2000.
12. Source: www.gidos.org, 6-11-2000.
13. Paul Zavidniak, Logicon Inc.:’Achieving Information Resiliency in the Defence Environment’, Information and Security and Data Security Congress , February 2000.
14. Amoroso, ‘Intrusion Detection: an introduction to Internet surveillance, correlation, traps, trace-back, and response’, intrusion.net books, 1999.
15. Sommer, ‘Intrusion Detection Systems as Evidence’, 1998, source: http://www.raid-symposium.org/raid98/Prog_RAID98/Table_of_content.html, 6-11-2000.
16. Allen J. e.a., ‘State of the Practice of Intrusion Detection Technologies’, January 2000, Technical Rapport CMU/SEI-99-TR-028; ESC-99-028.
17. Paxson, Handley, ‘Defending against NIDS evasion using traffic normalizers’, RAID ’99, Computer Networks, volume 34, number 4, 2000.
18. Source: http://dev.whitehats.com/ids, 6-11-2000.
19. Spafford, Zamboni, ‘Intrusion Detection using Autonomous Agents’, RAID ’99, Computer Networks, volume 34, number 4, 2000.
20. Mell et al, ‘A denial-of-service resistant intrusion detection architecture’, RAID ’99, Computer Networks, volume 34, number 4, 2000.
21. Source: http://www.sdl.sri.com/emerald/project.html, 6-11-2000.
22. Lippmann, Cunningham, ‘Improving Intrusion Detection Performance using Keyword Selection and Neural Networks’, RAID ’99, Computer Networks, volume 34, number 4, 2000.
23. Michael, Ghosh, ‘Using Finite Automata to Mine Execution Data for Intrusion Detection’, RAID 2000 Proceedings, Lecture Notes in Computer Science, vol. 1907, Springer, 2000.
24. Ghosh, ‘A Real-Time Intrusion Detection System Based on Learning Program Behaviour’, RAID 2000 Proceedings, Lecture Notes in Computer Science, vol. 1907, Springer, 2000.
25. Farley, ‘Visualisation of Intrusion Detection Data’, source: http://www.raid-symposium.org/raid2000/program.html, 6-11-2000.
26. Toelle, Niggemann, ‘Supporting Intrusion Detection by Graph Clustering and Graph Drawing’, source: http://www.raid-symposium.org/raid2000/program.html, 6-11-2000.
27. Kim G.H., Spafford E.H., ‘Experiences with Tripwire: Using Integrity Checkers for Intrusion Detection’, source: www.cs.purdue.edu/coast/ids, 6-11-2000.
28. Crosbie, ‘Applying genetic programming to intrusion detection’, Proceedings of 1995 AAAI Fall Symposium on Genetic Programming, November 1995.
29. Hochberg, J.; Jackson, K.; Stallings, C.; McClary, J.; DuBois, D.; Ford, J.: NADIR: An automated system for detecting network intrusions and misuse, in *Computers and Security* 12 (1993) 3, May, pp. 253-248.
30. Kantzavelou, I. and S.K. Katsikas, An attack detection system for secure computer systems - Outline for the solution. In L. Yngström and J. Carlsen (eds.), in Information security in research and business: Proceedings of IFIP TC11 13th international conference on Information Security in Copenhagen, Denmark, 14-16 May 1997. Chapman & Hall, London, etc., 1997, pp. 151-163.
31. Lee, W., and S.J. Stoflo, ‘Data mining approaches for intrusion detection’. In: Proceedings of the 7th USENIX security symposium. San Antonio, 26-29 January 1998, pp. 79-93.

32. Bishop C.M., ‘Neural networks for pattern recognition’, Oxford University Press, 1995.
33. Bonifácio Jr., J.M., E.S. Moreira, A.M. Cansian and A.C.P.L.F. Carvalho, ‘An adaptive intrusion detection system using neural networks’, In: Proceedings of the IFIP SEC’98 conference Wien/Budapest. Chapman & Hall, August 1998.
34. Mounje, A. and B. Le Charlier, ‘Continuous assessment of a UNIX configuration: integrating intrusion detection and configuration analysis’. In: Proceedings 1997 Symposium on Network and Distributed System Security San Diego, 10-11 February 1997, IEEE, Los Alamitos, pp. 27-35.
35. Kosoresow, A.P. and S.A. Hofmeyer, ‘Intrusion detection via system call traces’. In: IEEE Software. IEEE, 1997, Vol. 14, no 5, pp. 35-42.
36. Sebring, M.M., E. Shellhouse, M.E. Hanna, R.E. Whitehurst, Expert Systems in Intrusion Detection, a Case Study, in Proceedings of the 11th National Computer Security Conference, Baltimore, 1990.
37. Kumar, S., ‘Classification and detection of computer intrusions’, PhD Thesis, Purdue University, 1995.
38. Porras, P.A., R.A. Kemmerer, Penetration State Transition Analysis - A Rule-based Intrusion Detection Approach, In 8th Annual Computer Security Applications Conference, 220-229, IEEE Computer Security Press, 1992.
39. Garvey, T.D, T.F. Lunt, Model based Intrusion Detection, in Proceedings of the 14th National Computer Security Conference, 372-185, 1991.
40. Ludovic M., ‘GASSATA, a Genetic Algorithm as an Alternative Tool for Security Audit Trails Analysis’, source: www.cs.purdue.edu/coast/ids, 6-11-2000.
41. Cannady J. , Mahaffey J. , ‘The Application of Artificial Neural Networks to Misuse Detection: Initial Results’, www.cs.purdue.edu/coast/ids.
42. Huang, X., Biondi, Ph., Linux Intrusion Detection system (LIDS), www.lids.org
43. IAP: Intrusion Alert Protocol, Gupta, Hewlett-Packard, IETF IDWG work-in-progress.
44. Hes, R. and Borking, J. (editors), ‘Privacy Enhancing Technologies’, 1998, A&V-11, NDPA, The Hague.

Appendix B — List of Acronyms

BPD	Boundary Protection Device
BPS	Boundary Protection Services
CIDF	Common Intrusion Detection Framework
CIDS	CIS IDS
CIS	Communication and Information System
CISL	Common Intrusion Specification Language
COA	Courses of Action
COTS	Commercial Of The Shelf
DARPA	Defense Advanced Research Projects Agency
DMZ	De-Militarised Zone
DNS	Domain Name Service
DoS	Denial of Service
FTP	File Transfer Protocol
GIDO	Generalised Intrusion Detection Object
GOTS	Government Of The Shelf
HIDS	Host IDS
HTTP	Hyper Text Transfer Protocol
IAP	Intrusion Alert Protocol
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IDWG	Intrusion Detection Working Group
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISL	Intent Specification Languages
ISO	International Organization for Standardization (www.iso.ch)
IST	Information Systems Technology
LAN	Local Area Network
MIT	Massachusetts Institue of Technology
NATO	North Atlantic Treaty Organisation
NGO	Non-Governmental Organisation
NIDS	Network IDS
NN	Neural Network
NNIO	Non NATO International Organisation
NNN	Non-NATO Nation
PET	Privacy Enhancing Technologies
PKI	Public Key Infrastructure
RTO	Research Technology Organisation
SMTP	Simple Mail Transport Protocol
TCP	Transport Control Protocol
TGIA	Task Group on Information Assurance
UDP	User Datagram Protocol
UN	United Nations
XML	eXtensible Markup Language

This page has been deliberately left blank

Page intentionnellement blanche

Appendix C — List of Definitions

Accuracy	The number of *correct alarms* divided by the number of *correct alarms plus false alarms*; is a parameter for the relative number of correct alarms.
Activity	Anything that can be collected by sensors and that can possibly be related to intrusions, either directly or indirectly.
Active alarm	The generic model includes IDSs that have (optional) active components that can generate automatic reactive control signals.
Anomaly detection	The ‘normal behaviour’ of a CIS is known and an intrusion is detected, when the activity differs in some sense from the normal behaviour.
Alarm-processing unit	The generic component of an IDS that pre-processes and analyses the activity collected by the sensors.
Alarm messages	Messages for sharing intrusion related information, in between sensor IDSs and the CIDS, within and also outside the CIS for example with NATO coalition partners’ networks.
All-band information	Any other information, then in-band information that can be used in correlation, including information from human intelligence sources.
Attack	A deliberate intrusion in a CIS.
Attacker	The person, group, organisation, or state that performs and/or is responsible for an attack.
CIDS	CIS IDS: the system for intrusion detection in a CIS.
Communication channel	Channel used for communication of alarm messages and messages for management control.
Completeness	The number of *correct alarms* divided by the number of *correct alarms plus false rejections*; is a parameter for the relative number of correct alarms.
Correct alarm	An intrusion has occurred, and the IDS generated an alarm
Correct rejection	No intrusion has occurred and the IDS has not detected an intrusion.
Decoy deception systems	Also known as honey-pots, are systems designed to look and act like a real component of a CIS, but in fact their real design purpose is to attract attackers.
Defender	The person, group or organisation (i.e. NATO agency or NATO nation) that is responsible for the target CIS.
External intrusions	All intrusions that originate at the external network side of the BPS and that pass through the BPS.
False alarm	No intrusion has occurred, but the IDS has (erroneously) detected an intrusion
False rejection	An intrusion has occurred, but the IDS has not generated an alarm
Honey pots	See decoy deception systems
Host activity	Activity present at hosts (including clients, servers and routers)
In-band information	All information from activity inherent to the target system.
In-band communication	The network that might be under attack is used for the IDS communication.
Information deception systems	These systems are lures to give false information to intruders
Internal Intrusion	All intrusions that originate within the internal CIS or BPS.
Intruder	The person, group, organisation or state responsible for an intrusion.
Intrusion	A deliberate or accidental unauthorised access to, activity against, and/or activity in, a CIS.
Intrusion Detection	The process of identifying that an intrusion has been attempted, will occur, is occurring, or has occurred.
Intrusion Detection Systems	Technical means that focus on the detection type of measures against intrusions in a CIS.
Intrusion patterns	Specify the features, conditions, arrangements and interrelationships among activity that leads to break-in or other misuse.
Knowledge database	Part of IDS where information about known intrusions and/or the normal behaviour of the activity is stored.
Local intrusion	An intrusion that originates at the same host as the target itself
Location of IDS	The location of the hardware part of the sensor of an IDS. This is the physical position of an IDS in the network.
Management control messages	In an environment with multiple IDSs, the management units will be able to co-operate, by sharing messages for management control.

Misuse detection	The (type of) intrusion is known and stored beforehand (as a so-called signature). An intrusion is detected when the activity matches the known intrusion signature.
Network activity	The activity present at the network.
Out-of-band communication	A separate network or communication community (e.g. virtual LAN) is used for the internal IDS communication and alarm communication.
Passive alarm	An IDS generates an alarm, which can be a log file message, a pop-up screen, a pager message and so on, or a combination thereof.
Raw IDSs	IDSs that scan the unprocessed raw data for key strings. The term raw is not used in a derogatory manner, but rather to identify that these IDSs usually deal with the raw data directly.
Rules	See Intrusion patterns.
Sensors	The generic components of an IDS that collect *activity*.
Sensor IDSs	The IDSs that collect activity at a location in the CIS environment In fact sensor IDSs are the sensor component of the CIDS.
Signatures	See Intrusion patterns.
Smart IDSs	IDSs that have logic implemented that understands the target protocol. They will parse the request and perform (optimised) signature matching based on known rules pertaining to the protocol.
Storage database	Part of IDS where the alarm-processing unit can store (information about) collected activity that can be of interest in the future.

Appendix D — Analyser Techniques

D.1 Anomaly detection

D.1.1 Threshold detection

Threshold detection, also known as summary statistics, is one of the most basic forms of anomaly detection. During a certain time interval, a single metric of activity is analysed (e.g. the number of (failed) login attempts in the past hour, or the number of deleted files in a day). If this metric rises above a certain threshold value, the IDS detects an intrusion.

Threshold detection deals with the description and comparison problem as follows:

- *Description problem*: Threshold detection uses a single metric for describing subjects. This solution provides low protection against all intrusions except for the more unsophisticated intrusions.
- *Comparison problem*: Threshold detection compares the metric during an interval with a predetermined threshold.

A simple example of a threshold detection system is Tripwire [27]. All (system) files in a system are associated with a cryptographic signature. Whenever this signature differs from a stored signature, a warning is given. The stored signatures are cryptographic signatures of the (system) files, from a time that the system was certainly not intruded, e.g. right after installation.

D.1.2 Profile-based detection

Whereas threshold detection describes subjects by a single metric, in profile-based detection, the IDS' analyser measures a number of activity related metrics. The event analyser can use a wide range of metrics, such as:

- the number of audit records processed for a user in one minute;
- the relative distribution of file accesses and I/O activities over the entire system usage for a particular user;
- the relative frequency of logins from each physical location;
- the total or relative usage of each application;
- the total or relative usage of each system command;
- the amount of CPU and I/O used by a particular user;
- the number of file accesses of files with a certain confidentiality level.

The combination of all these measures for a particular subject is called the *current profile* of that subject. The current profile is periodically compared with a *stored profile* (in some IDSs, the stored profile is periodically merged with the current profile to "train" the system with regard to new activity behaviour) deviate sufficiently, an intrusion is detected. Profile-based detection has to deal with the description and the comparison problem:

- *Description problem*: Profile-based detection uses multiple metrics for describing subjects. Determining a suitable set of metrics that accurately predicts or classifies intrusions, but that can also be efficiently processed, is a difficult problem. E.g. [28] uses a genetic algorithm approach to solve this problem.
- *Comparison problem:* if one has somehow selected the right set of metrics, how does one define "sufficient deviation" between the stored profile and the current profile?

For example the following solutions can be used for the comparison problem.

- Statistics;
- Rule-bases;
- Neural networks;
- Intent specifications.

D.1.3 Statistics-based solutions

Statistical approaches compare profiles as follows: each metric in the stored profile is compared with its corresponding metric in the current profile, and based on that comparison an *abnormality value* is generated. These abnormality values are then combined by a combination function into a single abnormality value for the profile. If this abnormality value is higher than a certain statistical derived threshold the IDS detects an intrusion.

> Example:
>
> *A stored profile consists of i metrics with values s_1 to s_i. A current profile is measured with values c_1 to $c_{i.}$. The abnormality values a_i for these metrics are defined for this IDS as the absolute difference between these metrics: $a_i = |s_i - c_i|$. In this IDS, not all metrics are equally important, therefore a set of weights w_1 to w_i are used for each parameter. In addition, large abnormality values are seen as much more important than small abnormality values, and the abnormality functions are therefore squared. The combination function for the profile's abnormality value then becomes: $A = w_1 a_1^2 + w_2 a_2^2 + ... + w_i a_i^2$*
>
> *If A is higher than a predefined threshold T, the IDS flags an intrusion.*

Statistical profile-based approaches have a number of inherent disadvantages [29]:

- *No temporal information:* Statistical measures are insensitive to the order of occurrence of events and may miss intrusions that are indicated by sequential interrelationships among events.
- *Gradual misbehaviour*: If the system "trains" itself to keep up with changing circumstances, intruders who are aware of the IDS can train the system to a point where behaviour once considered abnormal is now considered normal.
- *Sporadic user environments*: Some environments, such as banking systems, have users who perform the same task day after day, with very minor variations. These environments are therefore very suitable for profile-based approaches. In other environments, such as university computer networks, users will have much more chaotic behaviour, and simple statistical approaches may not be suitable.

A current research IDS using statistics-based solutions is Emerald [20].

D.1.4 Rule-based solutions

Whereas statistical profile-based detection uses statistical formulas to compare profiles, rule-based detectors use sets of rules. In theory, rule-based approaches are stronger, because rules have greater expressive power. Rule-based approaches, for instance, can theoretically cope with temporal information and chaotically behaving users. Statistical approaches have great difficulties with this type of behaviour.

Rules can be generated automatically from audit data, or entered manually, to express policies and expert information. Creating a good rule-set is not easy.

An example of a rule-based solution is ADS (Attack Detection System) [30]. Two levels of abstraction have been considered: user commands/programs and system calls.

User commands and programs had a number of severe difficulties:

- UNIX has over 400 different user commands: building a rule base constitutes a significant effort.
- Users can rename commands, which makes detecting these commands impossible.
- Programs are very difficult to take into account, as an almost infinite number of different programs exist.
- If programs such as editors are used, it is hard to detect at this level of abstraction whether these programs actually change files.

After considering these difficulties, it was decided to use UNIX system calls as events. Within the operating system UNIX commands and programs use system calls to request services from the kernel. The approach to use system calls was chosen because:

- There is only a limited amount of system calls, so a relatively complete rule base can be constructed.
- System calls cannot be renamed.
- User programs have to use system calls, and can be examined by these system calls.
- When files are edited, it is possible to detect at this level of abstraction whether the file is changed.

In [30] two types of system calls were examined:

1. Successful security-relevant system calls;
2. Unsuccessful system calls that return a security-relevant error code.

For a user a profile is defined (through a rule-base) for the types of allowed system calls and the number of calls for every type. If this profile rises above a critical value, ADS flagged a possible intrusion.

D.1.5 Neural networks-based solutions

Whereas statistical and rule-based approaches explicitly store and process profiles, neural networks use a more implicit approach. The basic approach is to train a neural net using activity. Once the neural net is trained, it constitutes the profile of that subject, and the fraction of incorrectly predicted next events measures the variance of the activity from the profile [31].

Advantages of neural networks (NN) [32] are:

- Self-adaptive: the neural networks can be trained on the normal profiles. This does not require any specific knowledge of the different metrics. A NN can automatically account for correlations between the various measures that effect the output.
- Can generalise: their response is relatively insensitive to minor variations of the input.
- Can abstract: they are capable of abstracting the essence of a set of inputs.
- Can efficiently deal with the changing characteristics of the subject.
- Can potentially operate very fast.

- The approach does not depend on statistical assumptions on the nature of the underlying data.
- A NN copes well with noisy data.

Drawbacks of an NN [32] are:
- The initial training period of an NN can be substantial.
- Difficult to test the quality of a NN.
- The profile of the behaviour is “distributed” over the neural network, and hence impossible to understand by, e.g., system administrators.

[33] gives a proposal to provide mechanisms for NN for the recognition of successful intrusions, as well as to provide the capacity to adapt in response to the changes in the intruder’s techniques. Important advantage is the adaptive incorporation of security expert knowledge (administrator).

D.1.6 Intent Specification Languages

Another form of describing normal activity is with the use of Intent Specification Languages (ISL). ISLs are capable of specifying the user intent. This can be very useful because the closer one can get to specifying a user’s intent, the easier it is to determine whether these intentions are legitimate or not. Intelligent security systems can utilise knowledge bases, which contain specific tasks (including malicious attacks) that users may want to perform when using the system.

D.1.7 Other techniques

- *Data mining:* to discover consistent and useful patterns of system features that describe program and user behaviour. The set of relevant system features is used to compute (inductively learned) classifiers that can recognise anomalies and known intrusions [31]
- *Expert systems*: a deductive system [34].
- *System call tracing:* analysing system call traces, in particular their structure during normal and anomalous behaviour. Analysis of the temporal ordering of these calls reveals that such anomalies are localised within traces and that normal program behaviour can be described compactly using deterministic finite automata [35].

D.2 Misuse detection

D.2.1 Static pattern recognition

This technique is identified in [36]. This is the simplest form of misuse detection. It is usually based on relatively simple pattern recognition systems searching for e.g. (sub)strings in network packets. If a specific (sub)string is found, an intrusion is detected.

D.2.2 Conditional probability

This technique is identified in [37]. Static pattern recognition always flags an intrusion when a certain signature is found. This is not always correct: some signatures only sometimes relate to an attack. The conditional probability approach therefore tries to determine the conditional probability that an intrusion occurs, given that a certain signature is seen. To calculate this probability, data from previous intrusions is needed, for example from event logs and audit data.

D.2.3 Production / expert systems

This technique is also identified in [36]. Expert systems can be used for symbolic deduction of the occurrence of an intrusion based on given data. The expert system approach has a number of difficulties:
- rule-based approaches have severe difficulties with the handling of sequential data;
- the expertise in the expert system is only as good as that of the security officer(s) whose experience is being modelled. There is no concerted effort by security experts to distil their knowledge in a comprehensive rule set;
- the technique can only detect known vulnerabilities.

D.2.4 State Transition Analysis

This technique is identified in [38]. In this approach, intrusions are represented as a sequence of state transitions of the target system. Successive states are connected by arcs that represent the events required for changing state. Attack patterns are constructed of a sequence of state transitions.

D.2.5 Model-based intrusion detection

This technique is identified in [39]. This method combines models of misuse with evidential reasoning. There is a database of intrusion scenarios, each of which comprises a sequence of behaviour making up the intrusion. At any given moment, a subset of these attack scenarios is considered as likely scenarios. The IDS then tries to substantiate or refute these scenarios given the audit trail. As evidence for some scenarios accumulates, while for others the evidence drops, the list of active models is updated. The evidential reasoning calculus built into the system permits one to update the likelihood of occurrence of the attack scenarios in the active models list.

Advantages of model-based intrusion:

- Based on a mathematically sound theory of reasoning, considering the presence of uncertainty. Expert systems have great difficulty in doing so.
- It can reduce processing by analysing for “coarse” events for non-active scenarios, and starting to analyse for more detailed events as a scenario becomes active.

A disadvantage is, that building the intrusion detection model becomes more difficult, as meaningful and accurate evidence numbers have to be assigned to the various parts of the model.

In [40] a model-based intrusion detection approach, with genetic algorithms is used. Experiments with this system, called GASSATA, show quite good results that validate for the genetic approach to security audit trial analysis.

D.2.6 Neural Network based misuse detection

In [41], NNs have been trained to recognise known intrusions. Within the scope of the experiments, the neural networks were able to identify intrusive patterns.

However [16] indicates the following unsolved problems in the approach:

- The NNs were trained on small example sets. Large example sets could result in non-convergence of the NNs.
- Training times for large data sets may be unacceptable high.
- The NNs provide no inside into the process of how conclusions are generated.
- The work in both [20,30] depends only on packet header information, this reduces the number of intrusions that the NN can be trained upon to recognise.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	RTO-TR-049 AC/323(IST-008)TP/15	ISBN 92-837-1079-7	UNCLASSIFIED/ UNLIMITED

5. Originator
Research and Technology Organisation
North Atlantic Treaty Organisation
BP 25, 7 rue Ancelle, F-92201 Neuilly-sur-Seine Cedex, France

6. Title
Intrusion Detection: Generics and State-of-the-Art

7. Presented at/sponsored by
the Information Systems Technology Panel (IST) Task Group on Information Assurance (IST/RTG-003).

8. Author(s)/Editor(s)	9. Date
Multiple	January 2002

10. Author's/Editor's Address	11. Pages
Multiple	50

12. Distribution Statement There are no restrictions on the distribution of this document. Information about the availability of this and other RTO unclassified publications is given on the back cover.

13. Keywords/Descriptors

CIS (Communication and Information Systems)
Coalition information sharing
Communications management
Communications networks
Computer information security
Computer networks
Computer security
Correlation techniques
COTS (Commercial Off The Shelf)
Data processing security
Data transmission
Defense systems
Denial of service attacks
Early warning systems
Electronic security
Electronic signatures
IDS (Intrusion Detection Systems)
IDS generic models
Information systems
International cooperation
Intrusion alarm system
Intrusion alarms
Intrusion detectors
Monitors
Network security
Protection
Protocols
Secure communication
Visualization techniques
Warning systems

14. Abstract

This report presents the generics and describes state-of-the-art of Intrusion Detection Systems (IDSs). The report also aims at highlighting some of the issues for use of co-operative IDSs in a coalition environment.

To facilitate the discussions and analysis, generic models are introduced. This includes the IDS generic model, where an IDS consists of sensor, management and alarm-processing components and optionally may have reaction, deception, and visualisation components. To show how IDSs can be deployed and operate at different locations in a Communication and Information System (CIS), a generic model based on the CIS architecture is introduced as well. Finally, these generic models are extended as a way to look at intrusion detection in a coalition environment.

The report describes and discusses IDS analyser techniques, examples of commercial products, standardisation efforts, and several issues regarding interoperability, management, performance, availability, and privacy. Furthermore IDSs are discussed in relation to early warning of an intrusion in a CIS, and the need for evidence collection after an intrusion has occurred.

The discussions and analysis show that IDSs are useful in detection of intrusions in a CIS, even though several black spots are identified. It is also shown that IDS deployment and co-operation in coalition environments still need a great deal of research, development, standardisation, together with policy and management considerations.

This page has been deliberately left blank

Page intentionnellement blanche

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION
BP 25 • 7 RUE ANCELLE
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@rta.nato.int

DIFFUSION DES PUBLICATIONS
RTO NON CLASSIFIEES

L'Organisation pour la recherche et la technologie de l'OTAN (RTO), détient un stock limité de certaines de ses publications récentes, ainsi que de celles de l'ancien AGARD (Groupe consultatif pour la recherche et les réalisations aérospatiales de l'OTAN). Celles-ci pourront éventuellement être obtenues sous forme de copie papier. Pour de plus amples renseignements concernant l'achat de ces ouvrages, adressez-vous par lettre ou par télécopie à l'adresse indiquée ci-dessus. Veuillez ne pas téléphoner.

Des exemplaires supplémentaires peuvent parfois être obtenus auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la RTO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus sur la liste d'envoi de l'un de ces centres.

Les publications de la RTO et de l'AGARD sont en vente auprès des agences de vente indiquées ci-dessous, sous forme de photocopie ou de microfiche. Certains originaux peuvent également être obtenus auprès de CASI.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr, (FIZBw)
Friedrich-Ebert-Allee 34
D-53113 Bonn

BELGIQUE
Coordinateur RTO - VSL/RTO
Etat-Major de la Force Aérienne
Quartier Reine Elisabeth
Rue d'Evère, B-1140 Bruxelles

CANADA
Services d'information scientifique pour la défense (SISD)
R et D pour la défense Canada
Ministère de la Défense nationale
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Defence Research Establishment
Ryvangs Allé 1, P.O. Box 2715
DK-2100 Copenhagen Ø

ESPAGNE
INTA (RTO/AGARD Publications)
Carretera de Torrejón a Ajalvir, Pk.4
28850 Torrejón de Ardoz - Madrid

ETATS-UNIS
NASA Center for AeroSpace Information (CASI)
Parkway Center
7121 Standard Drive
Hanover, MD 21076-1320

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72, 92322 Châtillon Cedex

GRECE (Correspondant)
Hellenic Ministry of National Defence
Defence Industry Research & Technology General Directorate
Technological R&D Directorate
D.Soutsou 40, GR-11521, Athens

HONGRIE
Department for Scientific Analysis
Institute of Military Technology
Ministry of Defence
H-1525 Budapest P O Box 26

ISLANDE
Director of Aviation
c/o Flugrad
Reykjavik

ITALIE
Centro di Documentazione Tecnico-Scientifica della Difesa
Via XX Settembre 123a
00187 Roma

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research Establishment
Attn: Biblioteket
P.O. Box 25, NO-2007 Kjeller

PAYS-BAS
NDRCC
DGM/DWOO
P.O. Box 20701
2500 ES Den Haag

POLOGNE
Chief of International Cooperation Division
Research & Development Department
218 Niepodleglosci Av.
00-911 Warsaw

PORTUGAL
Estado Maior da Força Aérea
SDFA - Centro de Documentação
Alfragide
P-2720 Amadora

REPUBLIQUE TCHEQUE
DIC Czech Republic-NATO RTO
VTÚL a PVO Praha
Mladoboleslavská ul.
Praha 9, 197 06, Česká republika

ROYAUME-UNI
Dstl Knowledge Services
Kentigern House, Room 2246
65 Brown Street
Glasgow G2 8EX

TURQUIE
Millî Savunma Başkanliği (MSB)
ARGE Dairesi Başkanliği (MSB)
06650 Bakanliklar - Ankara

AGENCES DE VENTE

NASA Center for AeroSpace Information (CASI)
Parkway Center
7121 Standard Drive
Hanover, MD 21076-1320
Etats-Unis

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
Royaume-Uni

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council
Document Delivery
Montreal Road, Building M-55
Ottawa K1A 0S2, Canada

Les demandes de documents RTO ou AGARD doivent comporter la dénomination "RTO" ou "AGARD" selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications RTO et AGARD figurent dans les journaux suivants:

Scientific and Technical Aerospace Reports (STAR)
STAR peut être consulté en ligne au localisateur de ressources uniformes (URL) suivant:
http://www.sti.nasa.gov/Pubs/star/Star.html
STAR est édité par CASI dans le cadre du programme NASA d'information scientifique et technique (STI)
STI Program Office, MS 157A
NASA Langley Research Center
Hampton, Virginia 23681-0001
Etats-Unis

Government Reports Announcements & Index (GRA&I)
publié par le National Technical Information Service
Springfield
Virginia 2216
Etats-Unis
(accessible également en mode interactif dans la base de données bibliographiques en ligne du NTIS, et sur CD-ROM)

ST JOSEPH
OTTAWA/HULL

Imprimé par St-Joseph Ottawa/Hull
(Membre de la Corporation St-Joseph)
45, boul. Sacré-Cœur, Hull (Québec), Canada J8X 1C6

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION
BP 25 • 7 RUE ANCELLE
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Telefax 0(1)55.61.22.99 • E-mail mailbox@rta.nato.int

DISTRIBUTION OF UNCLASSIFIED
RTO PUBLICATIONS

NATO's Research and Technology Organisation (RTO) holds limited quantities of some of its recent publications and those of the former AGARD (Advisory Group for Aerospace Research & Development of NATO), and these may be available for purchase in hard copy form. For more information, write or send a telefax to the address given above. **Please do not telephone**.

Further copies are sometimes available from the National Distribution Centres listed below. If you wish to receive all RTO publications, or just those relating to one or more specific RTO Panels, they may be willing to include you (or your organisation) in their distribution.

RTO and AGARD publications may be purchased from the Sales Agencies listed below, in photocopy or microfiche form. Original copies of some publications may be available from CASI.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Coordinateur RTO - VSL/RTO
Etat-Major de la Force Aérienne
Quartier Reine Elisabeth
Rue d'Evère, B-1140 Bruxelles

CANADA
Defence Scientific Information Services (DSIS)
Defence R&D Canada
Department of National Defence
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
DIC Czech Republic-NATO RTO
VTÚL a PVO Praha
Mladoboleslavská ul.
Praha 9, 197 06, Česká republika

DENMARK
Danish Defence Research Establishment
Ryvangs Allé 1, P.O. Box 2715
DK-2100 Copenhagen Ø

FRANCE
O.N.E.R.A. (ISP)
29 Avenue de la Division Leclerc
BP 72, 92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr, (FIZBw)
Friedrich-Ebert-Allee 34
D-53113 Bonn

GREECE (Point of Contact)
Hellenic Ministry of National Defence
Defence Industry Research & Technology General Directorate
Technological R&D Directorate
D.Soutsou 40, GR-11521, Athens

HUNGARY
Department for Scientific Analysis
Institute of Military Technology
Ministry of Defence
H-1525 Budapest P O Box 26

ICELAND
Director of Aviation
c/o Flugrad
Reykjavik

ITALY
Centro di Documentazione Tecnico-Scientifica della Difesa
Via XX Settembre 123a
00187 Roma

LUXEMBOURG
See Belgium

NETHERLANDS
NDRCC
DGM/DWOO
P.O. Box 20701
2500 ES Den Haag

NORWAY
Norwegian Defence Research Establishment
Attn: Biblioteket
P.O. Box 25, NO-2007 Kjeller

POLAND
Chief of International Cooperation Division
Research & Development Department
218 Niepodleglosci Av.
00-911 Warsaw

PORTUGAL
Estado Maior da Força Aérea
SDFA - Centro de Documentação
Alfragide
P-2720 Amadora

SPAIN
INTA (RTO/AGARD Publications)
Carretera de Torrejón a Ajalvir, Pk.4
28850 Torrejón de Ardoz - Madrid

TURKEY
Millî Savunma Başkanliği (MSB)
ARGE Dairesi Başkanliği (MSB)
06650 Bakanliklar - Ankara

UNITED KINGDOM
Dstl Knowledge Services
Kentigern House, Room 2246
65 Brown Street
Glasgow G2 8EX

UNITED STATES
NASA Center for AeroSpace Information (CASI)
Parkway Center
7121 Standard Drive
Hanover, MD 21076-1320

SALES AGENCIES

NASA Center for AeroSpace Information (CASI)
Parkway Center
7121 Standard Drive
Hanover, MD 21076-1320
United States

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
United Kingdom

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council
Document Delivery
Montreal Road, Building M-55
Ottawa K1A 0S2, Canada

Requests for RTO or AGARD documents should include the word 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of RTO and AGARD publications are given in the following journals:

Scientific and Technical Aerospace Reports (STAR)
STAR is available on-line at the following uniform resource locator:
http://www.sti.nasa.gov/Pubs/star/Star.html
STAR is published by CASI for the NASA Scientific and Technical Information (STI) Program
STI Program Office, MS 157A
NASA Langley Research Center
Hampton, Virginia 23681-0001
United States

Government Reports Announcements & Index (GRA&I)
published by the National Technical Information Service
Springfield
Virginia 22161
United States
(also available online in the NTIS Bibliographic Database or on CD-ROM)

Printed by St. Joseph Ottawa/Hull
(A St. Joseph Corporation Company)
45 Sacré-Cœur Blvd., Hull (Québec), Canada J8X 1C6

ISBN 92-837-1079-7